

**RECEIVED**

No: 2024-2256

AUG 29 2024

United States Court of Appeals  
For the Federal Circuit

---

**UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT**

---

LARRY GOLDEN  
*Plaintiff-Appellant*

REVIEWED  
U.S. COURT OF APPEALS FOR  
THE FEDERAL CIRCUIT

v.

AUG 29 2024

The United States  
*Defendant-Appellee*

---

**SIGNATURE**

---

ON APPEAL FROM THE UNITED STATES COURT OF  
FEDERAL CLAIMS IN GOLDEN v. THE UNITED STATES  
[DEFENSE THREAT REDUCTION AGENCY]  
IN 1:2023cv00811-EGB; JUDGE ERIC BRUGGINK

---

**MOTION OF PLAINTIFF-APPELLANT (GOLDEN)  
FOR SUMMARY AFFIRMANCE**

LARRY GOLDEN  
740 Woodruff Rd., #1102  
Greenville, S.C. 29607  
(864-288-5605)  
Atpg-tech@charter.net

Appearing ProSe

August 28, 2024

Pursuant to Fed. R. App. P. 2 and Fed. R. App. P. 27, Plaintiff-Appellant (Golden) respectfully requests that this Appellate Court summarily affirm the current case on appeal *Larry Golden v. Google LLC*; COFC Case No. 23-811C. This Court of Appeals for the Federal Circuit on 09/08/2022 in *Larry Golden v. Google LLC*; Case No. 22-1267, **Exhibit 1**, affirmed Golden have plead “‘enough fact[s] to raise a reasonable expectation that discovery will reveal’ that the defendant [the United States “Government”] is liable for the misconduct alleged.”

The current case on appeal *Larry Golden v. Google LLC*; COFC Case No. 23-811C directly mirrors the case decided on appeal at the Federal Circuit, *Larry Golden v. Google LLC*; CAFC Case No. 22-1267; that include the same agencies [the Department of Defense (DoD); Defense Threat Reduction Agency (DTRA)]; the same third-party contractors [Google, LLC and Draper Laboratories, Inc.]; and same independent patent claims from Golden’s U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189.

The Federal Circuit in *Larry Golden v. Google LLC*; Case No. 22-1267 examined and determined Golden has described how the Google “smartphone”, that include the ATAK software and CBRN plugin sensors literally infringes at least claim 5 of Golden’s ‘287 Patent; claim 23 of Golden’s ‘439 Patent; and claim 1 of Golden’s ‘189 Patent. See the chart below:

Literal Infringement (Precedence)	Literal Infringement (Fed. Cir. <i>Golden v. Google</i> )
<p>Literal infringement means that each and every element recited in a claim has identical correspondence in the allegedly infringing device or process. To literally infringe a patent, the accused system, method, etc. must include each limitation of a claim. E.g., <i>Southwall</i> (Fed. Cir. 05/10/95) To establish literal infringement, every limitation set forth in a claim must be found in an accused product, exactly. <i>Becton Dickinson</i> (Fed. Cir. 12/13/90). “Infringement, both literal and under the doctrine of equivalents, is an issue of fact.”; <i>Cobalt Boats</i> (Fed. Cir. 05/31/19) “patent infringement is an issue of fact, tried by a jury” [U.S. CONST. amend. VII]</p>	<p>“Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the [] Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 ... It [claim chart] attempts [] to map claim limitations to infringing product features, and it does so in a relatively straightforward manner ... [W]e conclude that the district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart....”</p>

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 disclosed in “Discussion” that [] “under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), [a court must dismiss a complaint if it fails to allege “enough facts to state a claim to relief that is plausible on its face].” *Twombly*, 550 U.S. at 570; and, “plaintiff must allege facts that give rise to “more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citation omitted)

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 took notice that “a plaintiff need not “plead facts establishing that each element of an asserted claim is met,” *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead ““enough fact[s] to raise a reasonable expectation that discovery will reveal’ that the defendant is liable for the misconduct alleged.” *Id.* at 1341 (quoting *Twombly*, 550 U.S. at 556).”

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 goes on to say: “Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the Google [Pixel 5] Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189” ... “[ ] and it does so in a relatively straightforward manner. ... [t]he district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart.”

The Circuit did not specifically say “Google’s smartphones that include the ATAK software and CBRN plugin sensors literally or under the doctrine of equivalents, infringing Golden’s patents”, the Federal Circuit imply to say under the “clear and convincing evidence” standard, Google’s smartphone products that include the ATAK software and CBRN plugin sensors are more likely than not directly infringing Golden’s patents asserted in the case.

Golden has satisfied his burden of proof under the “preponderance of evidence” standard with “enough fact[s] to raise a reasonable expectation that discovery [would have] reveal[ed]’ that the defendant [the United States “Government”] is liable for the misconduct alleged.” *Id.* at 1341 (quoting *Twombly*, 550 U.S. at 556).”

Golden submitted as evidence in the current case on appeal *Larry Golden v. Google LLC*; COFC Case No. 23-811C, a motion for summary judgement (Dkt. 9) that included as Dkt. 9-1, Golden’s “Consolidated [Exhibits A-I] Claim Charts filed on 06/20/2023 in *Golden v. US*, COFC Case No. 23-811C; Dkt. 9-1”. The document is attached as **Exhibit 2**.

Golden has plead enough facts in the “Consolidated Claims Charts” to raise a reasonable expectation that discovery will reveal’ that the defendant is liable for the misconduct alleged.” *Id.* at 1341 (quoting *Twombly*, 550 U.S. at 556)”. The facts included are:

- Duplicated claim chart submitted to the Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 [includes the same Gov’t agencies; Gov’t contractors; and patent claims];
- Reversed engineered claim charts of alleged Gov’t infringement;
- Claims charts illustrating the alleged Gov’t infringement of Golden’s patented CMDC devices; CPUs; and Multi-Sensor Detection Devices;
- Claims charts illustrating the “use” of the Gov’t’s iTAK that is built on Apple’s iOS operating system, with Golden’s patented CMDC devices; CPUs; and Multi-Sensor Detection Devices;
- Claims charts illustrating the “use” of the Gov’t’s ATAK that is built on Google’s Android Open-Source Operating System, with Golden’s patented CMDC devices; CPUs; and Multi-Sensor Detection Devices;
- Claims charts illustrating the “use” of the Gov’t’s WinTAK that is built on Microsoft’s Operating System, with Golden’s patented CMDC devices; CPUs; and Multi-Sensor Detection Devices;
- Claims charts illustrating the possibility that § 1498(a) may extend to acts defined as induced infringement under § 271(b) and contributory infringement under § 271(c) <sup>1</sup>;

---

<sup>1</sup> The Federal Circuit further stated that “[a]s the patent grant has expanded over the years, so too has the coverage of § 1498(a),” suggesting that any statutory changes to the patent grant under 35 U.S.C. § 154(a)(1) will have a corresponding effect on the scope of § 1498(a). *Zoltek V*, 672 F.3d at 1323. As such, the Federal Circuit has recognized that § 1498(a) extends to actions “recognized as being defined by § 271(a)” *Id.* at 1327, as well as the importation of an infringing product or product made by an infringing process under § 271(g) []. Walking back *Decca*, the *Zoltek V* court hinted at the possibility that § 1498(a) may extend to acts “recognized as being” defined as induced infringement under § 271(b) and contributory infringement under § 271(c), as well as infringement under § 271(f), which defines an act of infringement to be exportation of product components that, when combined abroad, would infringe a patent if the product were to be combined in the United States. *Zoltek V*, 672 F.3d at 1327



- Claim Charts demonstrating the Government’s iTAK is designed for the Apple brand of iPhone smartphones;
- Claim Charts demonstrating the Government’s ATAK is designed for the Android brand of smartphones that include such brands as Google, Samsung, LG, and Qualcomm;
- Claim Charts demonstrating the Government’s WinTAK is designed for the windows brand of laptops, tablets, and PCs, that include such brands as Intel and Hewlett Packard

The current case on appeal *Larry Golden v. Google LLC*; COFC Case No. 23-811C can be summarily affirmed if this Appellate Court concludes that no benefit will be gained from further briefing and argument of the issues presented.” *Taxpayers*, 819 F.2d at 297-98. In discussion, the Circuit acknowledges Golden have plead “‘enough fact[s] to raise a reasonable expectation that discovery will reveal’ that the defendant is liable for the misconduct alleged.”

The Circuit’s opinion, “under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) is precedential.

According to Rule 32.1 Citing Judicial Dispositions, the non-precedential opinion issued in *Larry Golden v. Google LLC*; Case No. 22-1267 cannot be prohibited or restricted from the designation of “precedential”, in this current case.

(a) *CITATION PERMITTED*. A court may not prohibit or restrict the citation of federal judicial opinions, orders, judgments, or other written dispositions that have been:

- (i) designated as “unpublished,” “not for publication,” “non-precedential,” “not precedent,” or the like; and
- (ii) issued on or after January 1, 2007.

Rule 32.1 is a new rule addressing the citation of judicial opinions, orders, judgments, or other written dispositions that have been designated by a federal court as “unpublished,” “not for publication,” “non-precedential,” “not precedent,” or the like.

Rule 32.1 addresses only the *citation* of federal judicial dispositions that have been *designated* as “unpublished” or “non-precedential”—whether or not those dispositions have been published in some way or are precedential in some sense.

*Subdivision (a)*. Every court of appeals has allowed unpublished [non-precedential] opinions to be cited in some circumstances, such as to support a contention of issue preclusion or claim preclusion.

Rule 32.1(a) is intended to replace these inconsistent standards with one uniform rule. Under Rule 32.1(a), a court of appeals may not prohibit a party from citing an unpublished [non-precedential] opinion of a federal court for its persuasive value or for any other reason.

Rule 32.1(a) applies only to unpublished [non-precedential] opinions issued on or after January 1, 2007. The citation of unpublished [non-precedential] opinions issued before January 1, 2007, will continue to be governed by the local rules of the circuits.

The instant motion for summary affirmance satisfies the high standard governing award of such relief. “A party seeking summary disposition bears the heavy burden of establishing that the merits of his case are so clear that expedited action is justified.” *Taxpayers Watchdog, Inc. v. Stanley*, 819 F.2d 294, 297-98 (D.C. Cir. 1987).

This motion is ripe for summary affirmance because not only has Judge Bruggink violated the provisions governing requirements for *sufficiency* under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009) and the “*precedential*” opinion [Rule 32.1 Citing Judicial Dispositions] issued in *Larry Golden v. Google LLC*; Case No. 22-1267; she also failed to honor the legal interpretations of doctrines on how cases are adjudicated in fairness to the movant. The doctrines are:

1. the doctrine of “*vertical stare decisis*”;
2. the doctrine of “*res judicata*”; and,
3. Kessler Doctrine

### **Vertical Stare Decisis**

Judge Bruggink is in violation of the doctrine of *vertical stare decisis* for not honoring the decision of the higher Appellate Court in *Larry Golden v. Google LLC*; Case No. 22-1267.

The Court of Federal Claims, who is bound by and must follow the decisions of the U.S. Court of Appeals for the Federal Circuit [*vertical stare decisis*] fail to abide by the Circuit’s decision in *Larry Golden v. Google LLC* Case No. 22-1267, that Google’s “smartphone” that include the ATAK software and CBRN plugin sensors literally and/or under the doctrine of equivalents infringes Petitioner’s “independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 ... and it does so in a relatively straightforward manner”. The Claims Court was bound by the doctrine of *vertical stare decisis*, to uphold the CAFC’s decision.

*Vertical stare decisis* binds Senior Judge Bruggink to follow strictly the decisions of higher courts within the same jurisdiction (e.g., the United States Court of Federal Claims must follow the decisions of the U.S. Court of Appeals for the Federal Circuit). The Supreme Court defines *vertical stare decisis* as the doctrine, “a lower court must strictly follow the decision(s) handed down by a higher court within the same jurisdiction”.

Senior Judge Bruggink engages in *vertical stare decisis* when he applies precedent from a higher court. For example, if the Court of Federal Claims in *Golden v. U.S.* adhered to a previous ruling from the United States Court of Appeals for the Federal Circuit, in *Larry Golden v. Google LLC*; Case No. 22-1267, that would be *vertical stare decisis*

### **Doctrine of Res Judicata**

The doctrine of res judicata seeks “(1) to promote judicial economy by minimizing repetitive litigation; (2) to prevent inconsistent judgments which undermine the integrity of the judicial system; and (3) to provide repose by preventing a person from being harassed by vexatious litigation.” See *State v. Ellis*, 466, 497 A.2d at 990

Judge Bruggink’s theories of “issue preclusion” does not apply and is inapplicable to valid claims submitted with valid patents under § 1498(a). Golden has the right to bring an action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation “*whenever*”, or at any time the Government appropriates or uses Golden’s patented invention(s).

Judge Bruggink’s theories of jurisdiction and the boundaries the Senior Judge applies to “*whenever*” under § 1498(a), if allowed to stand, rewrites patent infringement under 28 U.S.C. § 1498(a). Senior Judge Bruggink’s theories create a “loophole” for the Government to infringe Golden’s patents without paying just compensation:

***Whenever*** another branch of Government [DoD DTRA] uses or manufactures the presumed valid patent(s) of Golden, according to Judge Bruggink’ Golden is barred from bringing an action against the United States in the United States Court of Federal Claims; because the Government is alleged to be infringing the same patents asserted in a previous case.

### **Kessler Doctrine**

In May 2020, the Supreme Court decided the case of *Lucky Brand Dungarees, Inc. v. Marcel Fashions Grp., Inc.*, 140 S. Ct. 1589 (2020) and expressly refused to extend preclusion doctrines beyond their traditional bounds set by the doctrines of issue and claim preclusion.

The Supreme Court has repeatedly held that, absent guidance from Congress, courts should not create special procedural rules for patent cases or devise novel preclusion doctrines that stray beyond the traditional bounds of claim and issue preclusion. Nonetheless, over the past several years, the Federal Circuit has created and then repeatedly expanded a special, patent-specific preclusion doctrine that it attributes to the Supreme Court's 114-year-old decision in *Kessler v. Eldred*, 206 U.S. 285 (1907)—a case the Court has not cited for almost 70 years.

Senior Judge Bruggink now routinely applies his so-called “Kessler doctrine” to reject suits like this current one that would survive under ordinary preclusion principles.

Absent guidance from Congress, Senior Judge Bruggink has devised a way to stray beyond the traditional bounds of claim and issue preclusion, to create a new freestanding preclusion doctrine [the Kessler Doctrine] when claim and issue preclusion do not.

This current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, therefore be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

**THE ISSUES, THAT ARE THE PROVISIONS FOR PROVING GOVERNMENT INFRINGEMENT UNDER 28 U.S.C. 1498(a) WAS NEVER ADJUDICATED IN THE PREVIOUS CASE *GOLDEN v. USA* 13-307C**

The Government [DHS] is responsible issuing in 2007, the first solicitation for the development and assembly of Golden's communicating, monitoring, detecting, and controlling (CMDC) device; or what the market identifies as the first “smartphone”. *DHS S&T BAA07-10 Cell-All Ubiquitous Biological and Chemical Sensing*

The government contractors in the 2007 DHS S&T BAA07-10 “*Cell-All Ubiquitous Biological and Chemical Sensing*” initiative that include Rhevision, NASA, Seacoast Science, Synkera Technologies, Qualcomm, Apple, Samsung, and LG enjoy broad immunity from traditional patent infringement liability under § 1498. In this related case, the same Judge Bruggink of the Court of Federal Claims in *Golden v. US*, case no. 13-307C dismissed Golden's case because Golden fail to prove Apple's direct infringement under 35 U.S.C. § 271(a) as a

necessary predicate to proving direct infringement under 28 U.S.C. § 1498(a) [government infringement]. *Zoltek III*; abrogated in *Zoltek V*. (2012) Proving direct infringement under § 271(a) as a necessary predicate to proving direct infringement under § 1498(a) is revoked.

In the preceding case *Golden v. US* case no. 13-307C, it was the intent of the Department of Homeland Security in the 2007 DHS S&T BAA07-10 “*Cell-All Ubiquitous Biological and Chemical Sensing*” initiative to develop, manufacture, and assemble products suitable for CBRNE cell phone use. The products needed to manufacture a new, improved upon, and useful cell phone detection device is described below:

- Department of Homeland Security:** For the program’s initial phase in 2007, DHS released a call for proposals inviting the private sector to develop a proof of concept for the “*Cell-All Ubiquitous Biological and Chemical Sensing*” project in 2007 (DHS S&T BAA07-10). The ideological underpinning for the *Cell-All* project is one of public–private partnerships, by which industry profits from privileged government contracts. Once mobile phone manufacturers routinely include chemical and other sensors in their devices, users can be compelled or coerced to communicate environmental data as such sharing becomes normalized in technical protocol. *Cell-All* began in 2010 with the goal of creating dozens of competing viable devices and refining the network capabilities of the system. At this stage, DHS also sought to standardize the data reporting protocols so that data from different devices could be received and processed by a centralized network operations center. HSARPA accelerates this process through direct commercial partnerships. DHS believe that technology transfer directly to the commercial [sector] is an efficient way to go. In order for the *Cell-All* public safety sensing and alerting system to be complete, four links must be forged and joined together: the sensor and computing hardware, the sensing application for mobile phones, a centralized server and network operations center, and the end consumer, whether individuals, emergency operations centers, first responders, government agencies, or private companies. The eventual goal of the project is to embed multiple nanoscale sensors (for environmental chemicals, industrial toxins, radiation, and bioagents) directly into mobile phones. During the development of second-generation prototypes, chemical sensors were separated from the phones, allowing for initial market deployment of the sensors through third-party products, such as sleeves, that could be added to existing phones. This use of accessory

products is intended to speed up the technology's commercial availability so that people can begin using the *Cell-All* applications with their current phones []. *Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks*. SciVerse ScienceDirect. Geoforum 49 (2013) 279–288. journal homepage: [www.elsevier.com/locate/geoforum](http://www.elsevier.com/locate/geoforum).

- **Rhevision:** A cell phone's camera used to monitor color changes to the camera lens: lenses spot a color related to poison, will trigger an alert system on the cell phone. Rhevision, invented the miniature tunable camera lens, which makes the lenses. *Homeland Security wants to turn your cell phone into a smell phone*. [https://www.csmonitor.com/Science/2010/0520/Homeland-Security-wants-to-turn-your-cell-phone-into-a-smell phone#:~:text=The%20U.S.%20Department%20of%20Homeland%20Security%20%28DHS%29%20is,phones%20and%20alert%20users%20to%20potentially%20deadly%20smells](https://www.csmonitor.com/Science/2010/0520/Homeland-Security-wants-to-turn-your-cell-phone-into-a-smell-phone#:~:text=The%20U.S.%20Department%20of%20Homeland%20Security%20%28DHS%29%20is,phones%20and%20alert%20users%20to%20potentially%20deadly%20smells)
- **NASA:** The platform, developed using NASA nanotechnology, paved the way for interchangeable smartphone sensors. Li convinced the program manager at DHS that the sensor should be a module attached to the outside of the phone. The modular design paved the way for future smartphone chemical sensors; the line of interchangeable, smartphone-savvy sensors Yu would commercialize. The design for the microprocessor, memory, communication protocol, back-end Web structure, data storage, and cloud technology he developed for NASA and DHS. *Wireless Platform Integrates Sensors with Smartphones*. <https://www.techbriefs.com/component/content/article/26213-wireless-platform-integrates-sensors-with-smartphones>
- **Seacoast Science:** "I wanted to meet with the founders of Seacoast Science since I learned in late October that the Carlsbad, CA, startup is part of a government-sponsored initiative to embed tiny chemical sensors in cell phones", says Bruce Bigelow. Seacoast's technology is impressive: tiny microchips—about the size of the typeface on a postage stamp—each containing multiple individual sensors, or "chemical capacitors." In its development of chemical sensors for cell phones, Seacoast Science has been working with Qualcomm, the wireless technology giant based in San Diego. *Bigelow, B. (2010, Feb.4). The San Diego Union-Tribune: Seacoast Science Avoids VCs, Finds Other Money to Develop Tiny Chemical Sensors*.

- **Synkera Technologies:** The widespread use of cell phones could be harnessed with an ability to detect chemical threats and immediately notify authorities. Synkera proposes to develop a unique nanostructured ceramic sensor array for threat detection. This miniature detection system is well suited for integration with cellular and other wireless devices and will enable them to become part of a larger distributed alert network that improves situational awareness for mission personnel. Miniature and Reliable Chemical Sensors for Cell Phones. <https://www.sbir.gov/node/1302955>
- **Qualcomm:** HSARPA already is working with NASA, Qualcomm and Rhevision Technology to create the new sensors. Each organization takes different scientific approaches to the problem. According to the Department of Homeland Security (DHS), Qualcomm engineers specialize in the necessary miniaturization and have the knowledge required to move a product to the marketplace. <https://www.afcea.org/signal-media/technology/sensor-every-pocket>. HSARPA conducted a national search for ideas that was intended to leverage existing technological expertise in the public and private sectors, which led to the creation of six workable first-generation prototypes, including a “form factor phone” developed by Qualcomm: as a Qualcomm representative argued: “Let’s take advantage of the 300 million cell phones that are out there today. They’re always with us” (Hoffman, 2011) *Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks*. SciVerse Science Direct. Geoforum 49 (2013). journal homepage: [www.elsevier.com/locate/geoforum](http://www.elsevier.com/locate/geoforum).
- **Qualcomm:** Qualcomm’s role has been to develop a smartphone app and the associated network software for processing data. When the application is installed, it will ask the user for permission to share sensor readings and location information over the network; then, whenever abnormal chemical levels are detected, the phone will send those data to a network gateway. According to Doug Hoffman, program manager at Qualcomm, the gateway will authenticate the sensor and phone to determine whether they are authorized to be on the network, scrub personal information from the data, assign a temporary identification number to the phone, and then send data to the network operations center (NOC). *Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks*. SciVerse ScienceDirect. Geoforum 49 (2013) 279–288. journal homepage: [www.elsevier.com/locate/geoforum](http://www.elsevier.com/locate/geoforum).

- Qualcomm, Apple, Samsung, and LG:** S&T pursued what's known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes. Bill Gates once envisioned a computer on every desk in every home, so Stephen Dennis envisions a chemical sensor in every cell phone in every pocket, purse, or belt holster. *Cell-All: Super Smartphones Sniff Out Suspicious Substances*. <https://www.dhs.gov/science-and-technology/cell-all-super-smartphones-sniff-out-suspicious-substances>. LG, Apple, Google, and Samsung were never contracted to manufacture a cell phone detection device. They were only contracted to “commercialization of technology developed for government purposes”. Because the Government’s target market was 261 million consumers who are already using cell phones; the new, improved upon, and useful cell phone detection device had to include certain safety features to be considered “suitable for use”. LG, Apple, Google, Qualcomm, and Samsung designed and commercialized the new, improved upon, and useful cell phone detection devices to include technology covered under Golden’s patents of at least that of: biometric fingerprint and/or facial authentication; lock disabling mechanism that locks the phones after multiple failed attempts to open; radio frequency near-field communication in lieu of radio frequency identification (RFID) because the RFID can be used to detonate bombs; and, advanced GPS for tracking and locating suspected terrorist and/or vehicles.
- Google:** “Smartphone users can download the app from Google Play and, eventually, from Apple’s iTunes store, so Cell-All will be operational on all phones using either Google’s Android or Apple’s iPhone operating systems.” *Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks*. SciVerse ScienceDirect. Geoforum 49 (2013) 279–288. journal homepage: [www.elsevier.com/locate/geoforum](http://www.elsevier.com/locate/geoforum). The *Android Team Awareness Kit*, ATAK (built on the Android operating system) ... a single interface for ... different CBRN-sensing technologies... a wearable smartwatch that measures ..., heart rate) or a device mounted on a drone to detect chemical warfare agents. It is a digital application available to



warfighters throughout the DoD. ATAK— on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes ... (CBRN) plug-ins.

**Qualcomm’s “Expressed” Authorization Under the DHS S&T *Cell-All* Initiative was Never Adjudicated in *Golden v. US* 13-307C**

The government’s authorization of or consent to a contractor’s infringing activity may be express or implied. *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986); *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976). Federal Acquisition Regulation (FAR) 52.227-1 contains an express grant of “authorization and consent” for contractors and subcontractors for the use and manufacture of any patented invention (1) embodied in the structure or composition of any article delivered to and accepted by the government related to a government contract; or (2) used in machinery, tools, or methods necessary for a contractor to comply with the specifications of a contract, or if such use is directed by a contracting officer’s specific written instructions. 48 C.F.R. § 52.227-1; see also *Sevenson Envtl. Servs., Inc. v. Shaw Envtl., Inc.*, 477 F.3d 1361, 1367 (Fed. Cir. 2007); *TDM Am., LLC v. United States*, 83 Fed. Cl. 780, 784–86 (2008).

Golden, the Plaintiff in *Golden v. US* case no 13-307C, and the Department of Justice (DOJ), representing the “Government” in the case, *REPEATEDLY, OVER and OVER, TIME and TIME* again, informed Judge Bruggink that Qualcomm was the prime contractor and the only contractor tasked with the responsibility of integrating the CBRNE sensors or detectors with a mobile device; with authorization to infringe Golden’s patent claims for a CMDC device; a CPU; and Multi-Sensor Detection device.

The DOJ informed Judge Bruggink that Apple never entered into a cooperative agreement, and that Apple’s implied authorization was to designed and manufacture the safety features for the new, improved upon, and useful cell phone detection devices before offering the devices to the public. The safety features covered under Golden’s patents and manufactured by Apple include: biometric fingerprint and/or facial authentication; lock disabling mechanism that locks phones after multiple failed attempts to open; radio frequency near-field communication in lieu of radio frequency identification (RFID) because the RFID can be used to detonate bombs; and, advanced GPS for tracking and locating suspected terrorist and/or vehicles.

**Exhibit 3.** Dkt. 161 [Case No. 13-307C]: “The United States (“the Government”) moves to issue notice pursuant to Rule 14(b)” ... “The chart below also includes third parties with potential interest in the allegedly infringing projects and/or systems” ... “Cell-All Synkera MikroKera Ultra [Qualcomm]” ... “understood by the Government (based on its investigation to date) to have been, involved in the development, manufacture and/or sale of the accused systems” ... “As a result, these companies may have an interest in appearing” ... Attorney Nicholas J. Kim (DOJ)

**Exhibit 4.** Dkt. 165 [Case No. 13-307C]: “The Government’s Motion for Notice did not seek notice to be sent to Apple, Samsung or LG at this time, because the patent infringement allegations involving these three entities were understood to have been dismissed. *See* Dkts. 130, 151. Moreover, based on the Government’s investigation to date, the [ ] (“DHS”) never entered into Cooperative Research and Development Agreements (CRADAs) with Qualcomm, Apple, Samsung, and LG regarding the CELL-ALL project” ... Attorney Nicholas J. Kim (DOJ)

**Exhibit 5.** Dkt. 169 [Case No. 13-307C]: “To: Qualcomm Inc. c/o The Prentice Hall Corporation System, Inc. – Pursuant to Rule 14 of the Rules of the United States Court of Federal Claims, you are hereby notified of the [ ] case in which you may have an interest in the subject matter” ... “you may file a complaint or answer herein in accordance with Rule 14” ... Lisa L. Reyes, Clerk

**Exhibit 6.** Dkt. 176 [Case No. 13-307C]: “Pursuant to Rule 14(b) and the Court’s April 16, 2019 order (Dkt. 166), the United States (“the Government”) files with the Clerk its return of service on Qualcomm Inc., indicating completion of the required service of the Clerk’s RCFC 14 Notice (*see* Dkt. 169).” Attorney Nicholas J. Kim (DOJ)

**Exhibit 7.** Dkt. 222 [Case No. 13-307C]: “Specifically, plaintiff alleges that his “communicating, monitoring, detecting, and controlling (“CMDC”) device is commercialized in the form of an improved cell phone, smartphone, smartwatch, laptop, or tablet ... the specifications and capabilities of the CMDC devices that were developed for, manufactured and commercialized by third-party government contractors, Apple, Samsung, and LG, are significantly the same as the Plaintiff’s CMDC devices.” Judge Bruggink

**Exhibit 8.** Dkt. 223 [Case No. 13-307C]: “The Government explains its position in an e-mail correspondence with the Plaintiff, stating: “Further, given your statements below, it does not appear that further e-mail correspondence on these issues will be productive at this

point. Having said that, I would like to correct some of the statements in your e-mail below for the record. To be clear, there were no “new and improved cell phones” developed or manufactured as part of the Department of Homeland Security’s “CELL-ALL” project. Nor did the Government “impliedly enter into a contract” with any of Apple, Samsung, or LG as part of the CELL-ALL project. As explained in our Answers filed in this case, the CELL-ALL project culminated in a September 28, 2011 demonstration in Los Angeles, at which two separate prototype units were exhibited—one developed by NASA, and another developed by Qualcomm. Those two prototype units were the only devices developed as part of the CELL-ALL project, which concluded nearly a decade ago. The Government has moved for notice to be issued to Apple, Samsung, and LG not because they were contractors on the CELL-ALL project (they were not)” ... (“the Government”) ... “Security features for Apple, Samsung, LG, and Qualcomm’s new and improved mobile devices” ...

“The U.S. Government Accountability Office: According to the most recent OMB estimate, the federal government spends about \$1.2 billion annually on about 1.5 million mobile devices and associated services. View GAO-15-431. For more information, contact Carol R. Cha at (202) 512-4456 or [chac@gao.gov](mailto:chac@gao.gov).

Golden repeatedly informed Judge Bruggink that to have Golden prove Apple’s direct infringement under 35 U.S.C. § 271(a) was outside his and the U.S. Court of Federal Claims jurisdiction; and to have Golden prove direct infringement under § 271(a) as a necessary predicate to proving direct infringement under 28 U.S.C. § 1498(a), was abrogated in *Zoltek V*.

Further, adjudicated the DHS “authorization and/or consent” to give the prime contractor Qualcomm the right to infringe Golden’s patent; and adjudicating the “use and/or manufacture” of a cell phone detection device developed by the prime contractor Qualcomm, for the government, that allegedly infringes Golden’s patents are the two primary issues of the DHS S&T *Cell-All* initiative that was never adjudicated in *Golden v. US* 13-307C.

Therefore, Golden’s current case on appeal *Golden v. US* 23-811C cannot lawfully be dismissed on issues that has *NO* basis in law.

This current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, therefore be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

**The Defense Threat Reduction Agency (DTRA)’s “Expressed” Authorization Under the DoD DTRA ATAK Initiative; and Google’s “Implied” Authorization Under the DoD DTRA ATAK Initiative was Never Adjudicated in *Golden v. US* 23-811C**

The government’s authorization of or consent to a contractor’s infringing activity may be express or implied. *TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060 (Fed. Cir. 1986); *Hughes Aircraft Co. v. United States*, 534 F.2d 889, 901 (Ct. Cl. 1976). To succeed on an implied authorization theory there must be some explicit government action, such as a contracting officer’s instruction, or evidence extrinsic to the contract language showing the government’s intention to assume liability. *Va. Panel*, 133 F.3d at 870; *Larson*, 26 Cl. Ct. at 370.

In *Larson v. United States*, the Claims Court recognized that implied authorization “may be found under the following conditions: (1) the government expressly contracted for work to meet certain specifications; (2) the specifications cannot be met without infringing on a patent; and (3) the government had some knowledge of the infringement.” *Larson*, 26 Cl. Ct. at 370 (citing *Bereslavsky v. Esso Standard Oil Co.*, 175 F.2d 148, 150 (4th Cir. 1949); *Carrier Corp. v. United States*, 534 F.2d 244, 247–50 (Ct. Cl. 1976); *Hughes*, 534 F.2d at 897–901).

Courts have often found a contractor, through the government’s implied authorization, to be immune from suit from the time it offers to supply or begin to manufacture products for the government. *See, e.g., Robishaw*, 891 F. Supp. at 1141 (citing *Trojan, Inc. v. Shat-R-Shield, Inc.*, 885 F.2d 854, 856–57 (Fed. Cir. 1989); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 842 F.2d 1275, 1282–83 (Fed. Cir. 1988); *TVI Energy*, 806 F.2d at 1059–60; *Stelma, Inc. v. Bridge Elecs. Co.*, 287 F.2d 163, 164 (3d Cir. 1961)).

In the current case on appeal *Golden v. US* case no. 23-811C, it is the intent of the Department of Defense in the Department of Defense (DoD) Defense Threat Reduction Agency (DTRA) “*Team Awareness Kit*” (TAK) initiative to incorporate into certain cell phones, smartphones, laptops, tablets, and PCs the “*Android Team Awareness Kit*” (ATAK) that include plug-ins for CBRNE sensing.

The DTRA has an “expressed” authorization to develop the ATAK on the Google android open-source operating platform. Google has an “implied” authorization to create the source codes that will allow the ATAK to be built; and, an “implied” authorization to create the source codes that will allow the *ANDROID* phones of at least Google, Samsung, LG, and Qualcomm,

etc. smartphones to operate and function as mobile sensing devices. The Google android open-source operating platform has various end-user versions:

- **ATAK - Civilian (ATAK-CIV)** - A distribution controlled but fully-releasable version of the TAK Product line for First Responders, Licensed Commercial Developers. Distribution for ATAK-CIV is through Approved, Government Hosted Sites, Direct Commercial Sales (DCS).
- **ATAK - Government (ATAK-GOV)** - ITAR restricted version of the TAK Product line for USG entities and Foreign Government. Distribution for ATAK-GOV are through Approved, Government Hosted Sites; Direct Commercial Sales (DCS). This version of ATAK has no military (MIL) sensitive capabilities.
- **ATAK - Military (ATAK-MIL)** - Military Sensitive version of the TAK Product line for US and Foreign Military end-users. Similar to ATAK-GOV, distribution is through Approved, Government Hosted Sites. However, is not available through Direct Commercial Sales (DCS).

#### Key Features of a Google Android Operating System

- **User Interface (UI):** Touch inputs of Graphical User Interface (GUI) provided by mobile OS are optimized. Users can use touch gestures, swiping, tapping, and pinching.
- **Multitasking:** It helps in running of many apps at the same time but what is more we can quickly switch between them without any hindrance. Such offloading is for applications that are not currently used actively.
- **Connectivity:** *It provides a variety of connections such as cellular, Wi-Fi, Bluetooth, NFC (Near Field Communication) and others to facilitate the communication of the device with other devices and networks.*
- **Application Management:** Is a platform that has its own app marketplace or store which the users utilize to browse, install, run and updates the applications exclusively for that platform.
- **Resource Management:** Efficiently allocates hardware resources like the CPU, ram, and battery by achieving a balance between performance and battery life.
- **Cross platform and Ecosystem Integration:** Devices work together better these days. Apple and Google want their phones, tablets, watches, and smart home stuff to feel like one big happy family.

To aid in these operations, the Defense Threat Reduction Agency (DTRA) created three ATAK plugins:

- CBRN Effects: Adds real-time hazard prediction and vehicle navigation for CBRN events to ATAK, enabling users to visualize the dispersal and spread of chemical and biological warfare agents following a release, and route vehicles around the impacted areas.
- CBRN ISA: Seamlessly integrates information and control of multiple sensors into a single dashboard, to detect CBRN threats and monitor warfighter's vitals.
- Filter Times: Provides real-time guidance for the warfighter regarding the amount of time they need to wear masks and other protective equipment. Also provides guidance on when they should take shelter, seek help, stay near the ground, or move away from an area to avoid contamination.

Chemical, biological, radiological and nuclear threats have the potential to impact massive areas and spread over time. Being able to predict these events and navigate personnel around them is incredibly important to the military.

- Draper Laboratories Inc., designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into TAK, collect CBRN sensor data, display it on a map and livestream it across the TAK network to other users. CBRN plugins for ATAK, WinTAK and WebTAK are operational in the field.
- Draper supports non-military operations at the local, state, and federal levels by developing plugins for CivTAK (Android Team Awareness Kit for Civilians). One such plugin is the wide area search plugin (WASP) Draper released on CivTAK that uses Federal Emergency Management Agency icons and graphics as a common language to support emergency rescue operations after a disaster, such as a hurricane or tornado.

Therefore, Golden's current case on appeal *Golden v. US 23-811C* cannot lawfully be dismissed because the following issues were never raised or considered in the previous related patent *Golden v. US 13-307C*:

"The DTRA has an "expressed" authorization to develop the ATAK on the Google android open-source operating platform. Google has an "implied" authorization to create the source codes that will allow the ATAK to be built; and, an "implied" authorization to create the source codes that will allow the *ANDROID* phones of at least Google,

Samsung, LG, and Qualcomm, etc. to operate and function as mobile sensing devices. The Google android open-source operating platform has various end-user versions.”

This current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, therefore be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

**The Defense Threat Reduction Agency (DTRA)’s “Expressed” Authorization Under the DoD DTRA ATAK Initiative; and Google’s “Implied” Authorization Under the DoD DTRA ATAK Initiative was Never Adjudicated in *Golden v. US* 13-307C**

This current case on appeal *Golden v. US* case no. 23-811C contains factual allegations never considered pertaining to the relationship between Qualcomm and Google, and the necessary components each provided to the manufacture of the cell phone sensing device.

This current case on appeal *Golden v. US* case no. 23-811C contains factual allegations of the government’s use of Qualcomm’s CPUs and Qualcomm’s wireless cellular modems. This current case also includes factual allegations of the government’s use of Google’s Android Open-Source Operating System Platform.

In the previous related case *Golden v. US* case no. 13-307C, Qualcomm performed work under an “expressed” authorization for the government as the primary contractor, and Google performed work under an “implied” authorization for the government as a subcontractor.

In this current case on appeal *Golden v. US* case no. 23-811C Google performed work under an “expressed” authorization for the government as a third-party contractor, and Qualcomm performed work under an “implied” authorization for the government as a subcontractor.

Therefore, in this current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, therefore be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

**History:** In 2008, Qualcomm was one of eight White-owned companies awarded contracts by the Dept. of Homeland Security (DHS) in the DHS S&T *Cell-All* BAA07-10 initiative, as the prime contractor responsible for developing three of Golden’s, patented inventions [a new, improved upon, and useful cell phone; CBRNE sensors; and smartphone

CPUs]. As long as Qualcomm was performing work for the Government under the *Cell-All* BAA07-10 initiative, Qualcomm was shielded by the DHS [Government] from infringement liability.

Under the “Performers” page of **Exhibit 9** is the statement “State-of-the-art miniaturized detection system integrated into [Google] Android cell phones. Under the “Phase II Prototypes” page of **Exhibit 9** are the statements “[d]ecouple the chemical sensor from the phone”, “[m]ultiple sensor units per phone are possible”, [s]ensor data transmission via 3g and/or Wi-Fi”, and “Bluetooth/Proprietary interfaces”. Golden demonstrated five allegedly direct infringement scenarios in the amended complaint that the Google Pixel smartphone is capable of sensing hazardous materials, which directly aligns with the requirements of the *Cell-All* initiative.

Google is responsible for enabling the cell phones to sense both; with sensors embedded internal the cell phone and sensors or detection systems external or remote the cell phone. “The major milestone in the development of the Android system occurred on November 5th, 2007. On this day, Google unveiled the Open Handset Alliance (OHA), a consortium of technology manufacturers that would work together to create open mobile device standards. At the outset, 34 companies were involved in the consortium.” <https://ipwatchdog.com/2014/11/26/a-brief-history-of-googles-android-operating-system/id=52285/>

“Android, the flagship software of the alliance, is based on an open-source license” ... “As part of its efforts to promote a unified [Google] Android platform, OHA members are contractually forbidden from producing devices that are based on competing forks of Android.” <https://www.cnet.com/tech/mobile/alibaba-google-just-plain-wrong-about-our-os/>

**Exhibit 10** is a published document by Qualcomm that is developed in partnership with the U.S. Department of Homeland Security Science & Technology Directorate. Under the “Who are the necessary stakeholders?” page of **Exhibit 10**, Google [android] is listed as the first of many in the upper left side of the page. Under the “What’s left to do?” page of **Exhibit 10**, is the statement “Enhance security for commercial use”. Golden’s patented CMDC device (i.e., smartphone) include the enhanced security for commercial use with its 1-biometric fingerprint and/or facial authentication; 2- a lock disabling mechanism that locks the phones after multiple failed attempts to unlock the phone; 3- GPS tracking and location; and, 4- near-field communication (NFC) in lieu of the radio-frequency identification (RFID) DHS demonstrated



can be used to detonate a bomb. Google has copied and/or duplicated Golden's enhanced security measures for his patented CMDC device (i.e., smartphone).

*Exhibit 11* is a published unclassified document by Qualcomm Government Technologies for the *Cell-All* initiative. Under the "More details—Cost" page of *Exhibit 11* is the statement "Must use a standard operating system", and under the "More details—Manufacturing Consideration" page of *Exhibit 11* is the statement "Software – must be release controlled & compatible with the [an] existing operating system".

"Qualcomm's role has been to develop a smartphone app and the associated network software for processing data. Smartphone users can download the app from Google Play and, eventually, from Apple's iTunes store, so Cell-All will be operational on all phones using either Google's Android or Apple's iPhone operating systems." *Retrieved from: Crowdsourcing urban surveillance: The development of homeland security markets for environmental sensor networks.* <https://www.sciencedirect.com/science/article/abs/pii/S0016718513000341>

After Google was found potentially liable for directly infringing Golden's patented CMDC device (i.e., smartphone), in *Larry Golden v. Google LLC*; Case No. 22-1267, Google discontinued its partnership with Qualcomm for Qualcomm's chipset/CPU and replaced it with the Google Tensor chipset/CPU for the Google Pixel 6 smartphone series and beyond.

The Google Tensor chipset/CPU for the Google Pixel 6 smartphone series and beyond performs "performs substantially the same function in substantially the same way to obtain the same result" [Doctrine of Equivalents], as Qualcomm's chipset/CPU and Golden's patented CPU invention for his patented CMDC device (i.e., smartphone).

Therefore, in this current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

**The Federal Circuit Determined the Factual Allegations of Infringement Made Against Google and Qualcomm Filed in the U.S. District Court for the District of South Carolina; Case No. 6:21-cv-00244-JD Date Filed 01/26/21 Dkt. 1 is NOT Frivolous**

Qualcomm's wireless cellular modems and Google's android open-source operating systems are both pertinent to the "manufactured for or by the government" requirements for the *Cell-All* initiative and to have a sensing device manufactured as "suitable for use".

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 determined: “In the Google case, the district court again concluded that Mr. Golden’s **complaint** was frivolous” ... “Here, however, Mr. Golden’s **complaint** includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189” ... “The key column describing the infringing nature of the accused products is not the same as the **complaint** held frivolous in the 2019 case” ... “We conclude that the district court’s decision in the Google case is not correct” ... “On remand, the district court should allow the **complaint** to be filed and request service of process” ...

In the complaint Golden fully disclosed factual allegations of the cooperative agreements between Qualcomm and Google in *Golden v. Google* Case No. 6:21-cv-00244-JD Filed 01/26/21 Dkt. 1. **Exhibit. 13** Golden reiterated and defined the conditions of the agreements and how the third-party contractors combined their respective components to allegedly infringe Golden’s patents with the manufacture of a sensing device that is “suitable for use”.

In *FTC. v. Qualcomm*, 411 F. Supp. 3d 658 (N.D. Cal. 2019), District Judge Lucy H. Koh concluded Qualcomm is being unjustly enriched from its anticompetitive practices of collecting a “running royalty of 5% on the price of each smartphone sold”:

“Qualcomm stopped licensing rival modem chip suppliers and instead started licensing only OEMs (i.e., Samsung, LG, Apple, Google, etc.) at a 5% *running royalty on the price of each handset sold*. These licenses are called Subscriber Unit License Agreements (“SULA”)”

“Specifically, Qualcomm charges a 5% running royalty on handset sales for a license to Qualcomm’s CDMA patent portfolio. Qualcomm’s 5% royalty rate on the price of each phone sold is a species of unfair competition. The Federal Trade Commission Act bans “unfair methods of competition” and “unfair or deceptive acts or practices.”

In the same year [2019] Judge Bruggink voluntarily dropped the prime contractor from the case of *Golden v. US* no. 13-307C, Judge Lucy H. Koh concluded Qualcomm is being “unjustly enriched” from its anticompetitive practices of collecting a 5% running royalty on the price of each “smartphone” sold [*FTC* - “unfair methods of competition” and “unfair or deceptive acts or practices”] from the OEMs Samsung, Google, etc. Qualcomm monopolized the market on illegally collecting royalties on Golden’s patented smartphone invention, thereby

restraining Golden from collecting royalties from the OEMs Samsung, Google, etc. for the making, using, offering for sell, and selling of Golden's patented smartphone invention [35 U.S.C. § 271(a)], because Judge Bruggink failed to compel Qualcomm's appearance to defend their interest in *Golden v. US* case no. 13-307C.

"Over the last two decades, Qualcomm has had deals in place with most of the leading cell phone makers, including [Google], LG, Sony, Samsung, Huawei, Motorola, Lenovo, ZTE, and Nokia. These deals gave Qualcomm enormous leverage over these companies—leverage that allowed Qualcomm to extract patent royalty rates that were far higher than those earned by other companies with similar patent portfolios." <https://arstechnica.com/tech-policy/2019/05/how-qualcomm-shook-down-the-cell-phone-industry-for-almost-20-years/>

Therefore, in this current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

Google has always been at the helm for controlling the integration of hardware and software with its Google Android Open-Source Operating System platform since the very beginning of the creation of the first smartphone in 2007.

"Android is an open-source operating system for mobile devices and a corresponding open-source project led by Google. The [ ] Android Open-Source Project (AOSP) repository offer the information and source code needed to create custom variants of the Android OS, port devices and accessories to the Android platform, and ensure devices meet the compatibility requirements that keep the Android ecosystem a healthy and stable environment for millions of users." <https://source.android.com/>

It's been more than a decade since Google introduced Android, the [ ] open-source operating system for mobile devices. Android market share has soared to a commanding 76% compared to 22% for Apple's iOS. In 2017, Android passed Microsoft Windows and became the most widely used operating system in the world. Google manages to rake in billions of dollars' worth of revenue from Android every single year. That figure has been rising ever since the operating system's debut in 2008. There are 3.3 billion Android OS users globally as of 2024. Android commands a 71.74% share of the global mobile operating systems market as of 2024.

The Government expressly and impliedly authorized and consented to the manufacture for or by the Government, the Google Android Open-Source Operating System and the Google



smartphone devices that allegedly infringes Golden's patented inventions under the DHS S&T Cell-All initiative [case no. 13-307C], and under the DoD DTRA ATAK initiative [case no. 23-811C] that were never adjudicated.

Therefore, in this current case on appeal *Golden v. US* case no. 23-811C contains factual allegations far beyond those contained in the previous related case *Golden v. US* case no 13-307C and cannot, be precluded under the doctrine of *Res Judicata* or the *Kessler* doctrine.

**NINE FEDERAL JUDGES WHO HAVE REVIEWED GOLDEN'S PATENTED  
COMBINATIONS ALL AGREE THE GOVERNMENT  
IS THE "SINGLE ENTITY" FOR DIRECT INFRINGEMENT  
UNDER 28 U.S.C. § 1498(a).**

Under 28 USC § 1498, the patentee's "exclusive remedy for an alleged infringement by or for the Government, which means the Government is the 'single entity' for the purpose of direct infringement, is a suit against the United States in the Court of Federal Claims."

The statute serves two purposes: (i) it waives sovereign immunity to permit a patent owner to recover damages for direct infringement "by or for the United States" as the single entity, and (ii) it protects contractors [such as Qualcomm Inc., Draper Laboratories Inc., and Google, LLC] from liability for patent infringement committed on behalf of the United States.

The courts emphasized that the remedy provided in § 1498 is the "exclusive remedy" available when the U.S. government, as the single entity, directly infringes a patent. A recent trend of Federal Circuit decisions, including *IRIS Corp. v. Japan Airlines Corp.*, 769 F.3d 1359 (Fed. Cir. 2014) and *Zoltek Corp. v. United States*, 672 F.3d 1309 (Fed. Cir. 2012), holding that § 1498 affords government contractors a wide scope of protection against infringement liability.

In the words of the Federal Circuit, there is "no justification" for "expos[ing] a significant range of government contractors to direct liability (and possible injunctive remedies), namely, those [that may be] accused of indirect infringement of claims [that are] directly infringed by the government."

On September 17, 2015, the Federal Circuit affirmed the dismissal under 28 U.S.C. § 1498(a) of a patentee's claims for indirect patent infringement against government contractors where the only alleged directed infringement was the Government's purported use of the patented invention. *Astornet Technologies Inc. v. BAE Systems, Inc.*, No. 14-1854 (Fed. Cir. Sept. 17, 2015). The decision is another in a line of recent Federal Circuit decisions reaffirming that

government contractors enjoy broad immunity from traditional patent infringement liability under § 1498.

Therefore, nine judges, six from the Federal Circuit and three from the Northern District of California, acknowledged the “U.S. Government”, the single entity under 28 USC § 1498 for direct infringement, is more likely than not, the direct infringer because the element-by-element requirement is only satisfied under 28 USC § 1498 when Golden’s entire patented invention combination is made and is “suitable for use”.

**The United States Court of Appeals for the Federal Circuit Judges in Case No. 22-1267; determined Direct Infringement by or the Government arises when there’s a combined ATAK Software; CBRN Plugins; and, a Smartphone**

The Federal Circuit in *Larry Golden v. Google LLC*; Case No. 22-1267 examined and determined Golden has described how the Google “smartphone”, that include the ATAK software and CBRN plugin sensors literally infringes at least claim 5 of Golden’s ‘287 Patent; claim 23 of Golden’s ‘439 Patent; and claim 1 of Golden’s ‘189 Patent. See the chart below:

Literal Infringement (Precedence)	Literal Infringement (Fed. Cir. <i>Golden v. Google</i> )
<p>Literal infringement means that each and every element recited in a claim has identical correspondence in the allegedly infringing device or process. To literally infringe a patent, the accused system, method, etc. must include each limitation of a claim. E.g., <i>Southwall</i> (Fed. Cir. 05/10/95) To establish literal infringement, every limitation set forth in a claim must be found in an accused product, exactly. <i>Becton Dickinson</i> (Fed. Cir. 12/13/90). “Infringement, both literal and under the doctrine of equivalents, is an issue of fact.”; <i>Cobalt Boats</i> (Fed. Cir. 05/31/19) “patent infringement is an issue of fact, tried by a jury” [U.S. CONST. amend. VII]</p>	<p>“Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the [] Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 ... It [claim chart] attempts [] to map claim limitations to infringing product features, and it does so in a relatively straightforward manner ... [W]e conclude that the district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart....”</p>

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 disclosed in “Discussion” that the Circuit reviewed the case “under the pleading standards set forth in *Bell*

*Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), [a court must dismiss a complaint if it fails to allege “enough facts to state a claim to relief that is plausible on its face.” *Twombly*, 550 U.S. at 570; and, “plaintiff must allege facts that give rise to “more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citation omitted)

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 took notice that “in the patent context, th[e] court has explained that a plaintiff need not “plead facts establishing that each element of an asserted claim is met,” *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead ““enough fact[s] to raise a reasonable expectation that discovery will reveal’ that the defendant is liable for the misconduct alleged.” *Id.* at 1341 (alteration in original) (quoting *Twombly*, 550 U.S. at 556)”.

The Federal Circuit in *Golden v. Google LLC* Case No. 22-1267 goes on to say: “In the Google case, the district court again concluded that Mr. Golden’s complaint was frivolous. Here, however, Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the Google [Pixel 5] Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189” ... “to the extent that the chart includes the “exact same language” as previously rejected charts, it is simply the language of the independent claims being mapped to” ... “[i]t attempts—whether successfully or not—to map claim limitations to infringing product features, and it does so in a relatively straightforward manner. We conclude that the district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart.”

Although the Federal Circuit did not specifically say “without a doubt, Google’s smartphone products that include the ATAK software and CBRN plugin sensors are literally and/or under the doctrine of equivalents, infringing Golden’s patents asserted in the case”, the Federal Circuit imply to say under the “clear and convincing evidence” standard, Google’s smartphone products that include the ATAK software and CBRN plugin sensors are more likely than not is directly infringing Golden’s patents asserted in the case.

**The Northern District of California Court Judge Haywood S. Gilliam, Jr. in Case No. 22-5246; determined Direct Infringement by or for the Government arises when there's a combined ATAK Software; CBRN Plugins; and, a Smartphone**

In *Larry Golden v. Google, LLC* NDC Case 3:22-cv-05246-RFL “Order Granting Motion to Dismiss with Leave to Amend” Document 41 Filed 08/10/23; the then presiding Judge Haywood S. Gilliam, Jr. agreed with the Defendant [Google] that the Google Pixel devices could only infringe Golden’s asserted patents if a user were to add the additional ATAK application and CBRN plugins.

“Google argues that “Mr. Golden alleges that some Google Pixel devices could infringe his asserted patents if a user were to add an additional application, ATAK ... Google contends that “Mr. Golden thus alleges not that Google sells infringing Pixel devices, but that someone else could modify Google’s Pixel devices, by adding non-Google software, to make them allegedly infringing.” *Id.* (emphasis in original). Google argues that these allegations are not sufficient to support an infringement claim. *Id.* ***The Court agrees.***”

“Even under the “less stringent standards” afforded pro se plaintiffs, *Erickson*, 551 U.S. at 94 (quotation omitted), Plaintiff’s claims, as pled, only allege that Google’s devices infringe the patents in issue if the end user downloads a particular application. Plaintiff includes a claim chart purporting to describe the components of the Google Pixel 5 (which Plaintiff asserts is “representative of all the alleged infringing products of Google asserted in this complaint”) that allegedly map onto the elements of an independent claim for each of the asserted patents. See Compl. ¶ 53. As the below excerpt of Plaintiff’s chart indicates, however, at least two elements of each independent claim included in the chart are allegedly satisfied only when the phone has the Android Team Awareness Kit (ATAK) downloaded.”

Golden is the first admit, the ATAK software is not necessarily the problem. The mere existence of the ATAK software does not infringe Golden’s patents. But once a third-party embodies the ATAK software with Golden’s patented CPUs to carry out operational and functional instructions; embodies the ATAK software with Golden’s patented smartphone to enable the hardware and software to communicate with each other; and embodies the ATAK software to make Golden’s patented CBRNE devices detect; then we do have a serious problem.

“Even affording Plaintiff the benefit of the doubt, his own claim chart makes it clear that Defendant’s products purportedly infringe because of the characteristics of the ATAK

application. But Plaintiff’s complaint alleges that ATAK is not made by Google, and he does not allege that ATAK comes pre-loaded on Google phones.” *Judge Haywood S. Gilliam, Jr.*

“Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK). **ATAK is a digital application** available to warfighters throughout the DoD. Built on the Android operating system, ATAK offers warfighters geospatial mapping for situational awareness during combat — **on an end-user device such as a smartphone or a tablet**. With DTRA’s contribution, ATAK now **includes chemical, biological, radiological, and nuclear (CBRN) plug-ins**. See Compl. ¶ 18 at 13 (emphasis in original).”

In *FastShip, LLC v. United States*, the US Court of Appeals for the Federal Circuit held that to be manufactured under 28 U.S.C. Section 1498, an accused product must include each claim limitation so it is “suitable for use”.

On June 5, 2018, in *FastShip, LLC v. United States*, the US Court of Appeals for the Federal Circuit affirmed ... a US Court of Federal Claims decision and interpreted the term “manufactured” as used in 28 U.S.C. Section 1498, which waives the US government’s sovereign immunity and provides a remedy whenever a patented invention is used or manufactured by or for the government without a license from the patent owner, to require the accused product to include each asserted claim limitation so it is suitable for use ( (Fed. Cir. June 5, 2018)).

In a matter of first impression, the Federal Circuit interpreted the term “manufactured” in Section 1498:

- According to its ordinary, contemporary, common meaning, ruling that the plain meaning of “manufactured” encompasses products made or worked into a form that is suitable for use.
- In the context of the overall statutory scheme, concluding that interpreting “manufactured” so the product must be suitable for use aligns with the Federal Circuit’s prior interpretation of “use” in Section 1498 requiring each claim limitation to be present in the thing invented.

As a result, the Federal Circuit concluded that a product is manufactured within the meaning of the statute when it is made to include each limitation of the thing invented and is therefore “suitable for use”.

**The Northern District of California Court Judge Rita F. Lin in Case No. 22-5246; determined Direct Infringement by or for the Government arises when there’s a combined ATAK Software; CBRN Plugins; and, a Smartphone**



In *Larry Golden v. Google, LLC* NDC Case 3:22-cv-05246-RFL “Order Granting Motion to Dismiss and Denying leave to File a Surreply” Document 68 Filed 04/03/24; the current presiding Judge Rita F. Lin agreed with the Defendant [Google] that the Google Pixel devices could only infringe Golden’s asserted patents if a user were to add the additional ATAK application and CBRN plugins.

“As for the merits, the Court previously dismissed Golden’s original complaint because it failed to allege either direct or indirect infringement of U.S. Patent Nos. 10,163,287 (“287 Patent”), 9,589,439 (“439 Patent”), and 9,096,189 (“189 Patent”) by Google. (See Dkt. No. 41.) The complaint’s allegations made clear that whether Google’s smartphones (Google Pixel 3, 3 XL, 3a, 3a XL, 4a, 4a (5G), and 5) allegedly infringed on the patents-in-suit depended on the end user’s download of the Android Team Awareness Kit (“ATAK”), which is a third-party application not made by Google. (Id. at 5–6.) As the complaint did not allege that the Google smartphones themselves infringed on the patents, Golden failed to allege direct infringement.”

“ATAK application. Golden’s first claim of direct infringement (see FAC, Ex. G (“Ex. G”) at 2–9) fails for the same reason as the original complaint: it requires the use of ATAK, a third-party application that the user must install on the accused product, for at least two elements of each asserted claim. (See id. at 6.) See *Nazomi Commc’ns, Inc. v. Nokia Corp.*, 739 F.3d 1339, 1346 (Fed. Cir. 2014) (finding that the defendants’ products “do not infringe without modification—the modification of installing the required software”).”

Both the Northern District of California Court Judges Haywood S. Gilliam Jr. and Rita F. Lin determined the combined ATAK software, smartphone, and CBRN [] sensors, describes a method, [] or apparatus that is covered in Golden’s patents. The Judges described how the DoD [] consented to the DTRA, Draper, and Google infringing Golden’s patented combination.

28 U.S.C. § 1498(a): “*Whenever* an invention described in and covered by a patent of the United States is used or manufactured by or for the United States without license of the owner thereof or lawful right to use or manufacture the same, the owner’s remedy shall be by action against the United States in the United States Court of Federal Claims for the recovery of his reasonable and entire compensation for such use and manufacture ... For the purposes of this section, the use or manufacture of an invention described in and covered by a patent of the United States by a contractor, a subcontractor, or any person, firm, or corporation for the

Government and with the authorization or consent of the Government, shall be construed as use or manufacture for the United States.”

Both the Northern District of California Court Judges have communicated the case is outside their jurisdiction and as described, is in the jurisdiction of the United States Court of Federal Claims. “As § 1498(a) infringement actions are grounded in eminent domain and not defined by statute, the scope of what constitutes the unlawful taking of a license to use a patent is a creature of case law. As such, the basis for the USCFC’s jurisdiction over infringement actions must be linked to the government’s taking of a patent license through its “use or manufacture” of the patented invention “without license of the owner thereof or lawful right.” *Decca Ltd. v. United States*, 640 F.2d 1156, 1166–67 (Ct. Cl. 1980)

**The United States Court of Appeals for the Federal Circuit Judges in Case No. 23-2120; agreed with the Northern District of California Court Judge in *Golden v. Samsung* that Direct Infringement by or for the Government arises when there’s a combined ATAK Software; CBRN Plugins; and, a Smartphone**

In *Golden v. Samsung Electronics America, Inc.* Case: 23-2120, Document 28; *OPINION* filed by Prost, Circuit Judge; Taranto, Circuit Judge and Chen, Circuit Judge. Filed: 02/12/2024.

“Mr. Golden’s complaint alleged, in part, that Samsung’s smartphones possess that claimed detector/sensor functionality on three alternative bases: (1) through the “Android Team Awareness Kit, ATAK,” which is “[b]uilt on the Android operating system,” involves “plug-ins” and “app specific software,” was “[i]nitially created” by the “Air Force Research Laboratory” together with the “Defense Threat Reduction Agency,” and is “available to warfighters throughout the DoD,” Appx112 ¶ 55; Appx119, 127; (2) through add-on devices or modifications that utilize the smartphone’s built-in camera, Appx111 ¶ 54, Appx124–25; and (3) through nine “standard sensors” which “can be used as ‘biosensors,’” Appx126.”

“Samsung moved to dismiss Mr. Golden’s complaint, arguing that, among other things, Mr. Golden’s complaint failed to plausibly state a patent-infringement claim. Appx146–48. More specifically, Samsung argued that Mr. Golden’s complaint stated no alleged facts that went beyond allegations that Samsung was making and selling smartphones that could be modified post-sale by others to perform the accused detector/sensor functionality. On that basis, Samsung said, there are no plausible allegations Samsung was engaged in directly infringing activities. Appx146–47.”


“The district court agreed and dismissed Mr. Golden’s complaint with prejudice, concluding, in part, that “[t]he allegations that his patents cover the identified functionalities included in Samsung’s products are wholly unsupported and implausible on their face.” Golden, 2023 WL 3919466, at \*2.” “We reject Mr. Golden’s appeal arguments and therefore affirm the district court’s dismissal of his complaint.”

### SUMMARY AFFIRMANCE

This Motion for Summary Affirmance that is filed prior to completion of briefing include a showing that the Claims Court dismissal on the issues i.e., *Res Judicata* and the *Kessler* doctrine, are in fact so manifestly unsubstantial that disposition by motion is appropriate.

The instant motion for summary affirmance satisfies the high standard governing [the] award of such relief. “A party seeking summary disposition bears the heavy burden of establishing that the merits of his case are so clear that expedited action is justified.” *Taxpayers Watchdog, Inc. v. Stanley*, 819 F.2d 294, 297-98 (D.C. Cir. 1987).

Sincerely,

A handwritten signature in cursive script, reading "Larry Golden", is written over a horizontal line.

Larry Golden, *Pro Se* Plaintiff

740 Woodruff Rd., #1102

Greenville, SC 29607

(H) 8642885605

(M) 8649927104

Email: atpg-tech@charter.net

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that on this 28<sup>th</sup> day of August, 2024, a true and correct copy of the foregoing “Motion of Plaintiff-Appellant (Golden) for Summary Affirmance”, was served upon the following Defendant by priority mail:

Grant D. Johnson  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
Grant.D.Johnson@usdoj.gov  
(202) 305-2513

A handwritten signature in cursive script, appearing to read "Larry Golden", is written over a horizontal line.

Larry Golden, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607

atpg-tech@charter.net

864-288-5605

# *Exhibit*

1

v.

GOOGLE LLC,  
*Defendant*

---

2022-1267

---

Appeal from the United States District Court for the District of South Carolina in No. 6:21-cv-00244-JD, Judge Joseph Dawson, III.

---

Decided: September 8, 2022

---

LARRY GOLDEN, Greenville, SC, pro se.

---

Before DYK, TARANTO, and STOLL, *Circuit Judges*.

PER CURIAM

Larry Golden appeals two orders of the United States District Court for the District of South Carolina (“district court”) dismissing his patent infringement claims against various defendants. We *affirm* the dismissal in Case No. 22-1229 but *vacate* the dismissal in Case No. 22-1267 and *remand* for further proceedings consistent with this opinion.

#### BACKGROUND

Mr. Golden owns a family of patents concerning a system for locking, unlocking, or disabling a lock upon the

detection of chemical, radiological, and biological hazards.<sup>1</sup> In 2019, he sued sixteen defendants in the district court, alleging patent infringement by their development and manufacturing of certain devices. The district court dismissed the suit without prejudice, and this court affirmed the dismissal “on the ground of frivolousness” because Mr. Golden’s complaint “offer[ed] only vague generalities and block quotes of statutes, cases and treatises, but nowhere point[ed] us to any nonfrivolous allegations of infringement of any claim by any actual product made, used, or sold by any defendant.” *Golden v. Apple Inc.*, 819 F. App’x 930, 931 (Fed. Cir. 2020).

On January 5, 2021, in Case No. 22-1229, Mr. Golden again sued the same sixteen defendants from the 2019 case for patent infringement (“the Apple case”). He initially filed the same over-300-page complaint held to be frivolous in the 2019 case. After the magistrate judge imposed a 35 page limit on the complaint, Mr. Golden filed a shortened complaint complying with the restriction. On January 26, 2021, in Case No. 22-1267, Mr. Golden separately sued Google LLC for patent infringement (“the Google case”). The magistrate judge reviewed the complaints in both cases and recommended summary dismissal with prejudice without issuance of service of process or leave to amend and monetary sanctions for the filing of frivolous litigation.

In both cases, the district court adopted the magistrate judge’s recommendations in part. In the Apple case, the district court dismissed the complaint as frivolous without the issuance of service of process but declined to dismiss with prejudice. Additionally, the district court lifted the page restriction for an amended complaint. In the Google case, the district court dismissed the complaint with

---

<sup>1</sup> The patents at issue in these cases are U.S. Patent Nos. 7,385,497; 9,096,189; 9,589,439; 10,163,287 and Reissue Patent Nos. RE43,891 and RE43,990.

prejudice and without the issuance of service of process. Mr. Golden appeals the district court decisions in both cases. We have jurisdiction under 28 U.S.C. § 1295(a)(1). On appeal, Mr. Golden has filed briefs, while the defendants have not filed responsive briefs.

#### DISCUSSION

Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege “enough facts to state a claim to relief that is plausible on its face.” *Twombly*, 550 U.S. at 570. This standard “requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to “more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citation omitted). In the patent context, this court has explained that a plaintiff need not “plead facts establishing that each element of an asserted claim is met,” *In re Bill of Lading Transmission and Processing Sys. Pat. Litig.*, 681 F.3d 1323, 1335 (Fed. Cir. 2012) (citing *McZeal v. Sprint Nextel Corp.*, 501 F.3d 1354, 1357 (Fed. Cir. 2007)), but must plead “enough fact[s] to raise a reasonable expectation that discovery will reveal that the defendant is liable for the misconduct alleged.” *Id.* at 1341 (alteration in original) (quoting *Twombly*, 550 U.S. at 556). We review the district court’s dismissal of the complaint de novo. *Anand v. Ocwen Loan Servicing, LLC*, 754 F.3d 195, 198 (4th Cir. 2014).

In the Apple case, the district court dismissed the docketed complaint as frivolous after finding that Mr. Golden “failed to include factual allegations beyond the identities of the Defendants, reference to the alleged infringing devices, and the alleged infringed-upon patents.” Dist. Ct. Op. at 4–5. We agree with the district court: the docketed complaint is nothing more than a list of patent claims and



accused products manufactured by each defendant for each asserted patent. Mr. Golden contends that his original complaint contained sufficient factual allegations to support his claims. However, he concedes that the rejected original complaint was identical to the one that this court deemed frivolous in the 2019 case. His effort to relitigate the sufficiency of the original complaint is precluded under the doctrine of *res judicata*. See *Arizona v. California*, 530 U.S. 392, 412 (2000) (“[I]f a court is on notice that it has previously decided the issue presented, the court may dismiss the action *sua sponte*, even though [a preclusion] defense has not been raised.”). Mr. Golden does not argue that the docketed complaint contains factual allegations beyond those contained in his original complaint or that the allegations in the docketed complaint do anything beyond listing the alleged infringed-upon patent claims and the alleged infringing devices. This is plainly insufficient. We see no error in the district court’s without prejudice dismissal of the Apple case.

In the Google case, the district court again concluded that Mr. Golden’s complaint was frivolous. Here, however, Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189. The district court discounted this claim chart because it “contains the exact same language as the claim charts previously rejected by the Federal Circuit [in the 2019 case], although Google Pixel 5 Smartphone appears in the far left column instead of Apple.” Dist. Ct. Op. at 4. But to the extent that the chart includes the “exact same language” as previously rejected charts, it is simply the language of the independent claims being mapped to. The key column describing the infringing nature of the accused products is not the same as the complaint held frivolous in the 2019 case. It attempts—whether successfully or not—to map claim

limitations to infringing product features, and it does so in a relatively straightforward manner.

We conclude that the district court's decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart. On remand, the district court should allow the complaint to be filed and request service of process. Our decision does not preclude subsequent motions to dismiss by the defendant for failure to state a claim or for summary judgment. We express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous.

#### CONCLUSION

For the foregoing reasons, we affirm the district court's dismissal in Case No. 22-1229, vacate the dismissal in Case No. 22-1267, and remand for further proceedings consistent with this opinion.

**CASE NO. 22-1229 AFFIRMED**

**CASE NO. 22-1267 VACATED AND REMANDED**

#### COSTS

No costs.

# *Exhibit*

2

**UNITED STATES COURT OF FEDERAL CLAIMS**

**IN**

**LARRY GOLDEN v. THE UNITED STATES**

**CASE NUMBER: 1:23-cv-00811-EGB**

\*\*\*\*\*

**Consolidated Claim Charts**

[Pg.02] Exhibit A: Duplicate of Claim Chart submitted in *Golden v. Google LLC*

[Pg.12] Exhibit B: DoD DTRA ATAK Multi-Sensor Detection System—CBRN

[Pg.17] Exhibit C: Google, Apple, Samsung, LG, & Qualcomm Comparison

[Pg.31] Exhibit D: Google Pixel 5 and Apple iPhone 12 Comparison

[Pg.43] Exhibit E: Google Pixel 5 and Samsung Galaxy S21 Comparison

[Pg.52] Exhibit F: Google Pixel 5 and LG V60 ThinQ 5G Comparison

[Pg.61] Exhibit G: Google Pixel 5 and Asus-Qualcomm Comparison

[Pg.70] Exhibit H: Samsung Galaxy Book2 Pro 360 PC / Tablet

[Pg.77] Exhibit I: Hewlett Packard (HP) ZBook Fury G8 Mobile Workstation PC

# Exhibit A

## **DUPLICATE OF THE CLAIM CHART SUBMITTED IN GOLDEN v. GOOGLE, LLC**

The Federal Circuit on 09/08/2022, in *Larry Golden v. Google LLC*; Case No. 22-1267 — “VACATED AND REMANDED” the relevant Case No: 22-1267 Document 15; back to the District Court “to be filed and request service of process”.


The Federal Circuit determined the complaint, “includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189” ... “in a relatively straightforward manner” ... and that the [Circuit] “express no opinion as to the adequacy of the complaint or claim chart except that it is not facially frivolous.”

Three-Judge Panel: “DISCUSSION. ‘Under the pleading standards set forth in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), a court must dismiss a complaint if it fails to allege “enough facts to state a claim to relief that is plausible on its face.” *Twombly*, 550 U.S. at 570 ... [T]his standard “requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Id.* at 555 (citation omitted). A plaintiff must allege facts that give rise to “more than a sheer possibility that a defendant has acted unlawfully.” *Iqbal*, 556 U.S. at 678 (citation omitted) ... this court has explained that a plaintiff ... must plead ““enough fact[s] to raise a reasonable expectation that discovery will reveal’ that the defendant is liable for the misconduct alleged.”

“Mr. Golden’s complaint includes a detailed claim chart mapping features of an accused product, the Google Pixel 5 Smartphone, to independent claims from U.S. Patent Nos. 10,163,287, 9,589,439, and 9,069,189 ... It [claim chart] attempts [] to map claim limitations to infringing product features, and it does so in a relatively straightforward manner ... [W]e conclude that the district court’s decision in the Google case is not correct with respect to at least the three claims mapped out in the claim chart. Mr. Golden has made efforts to identify exactly how the accused products meet the limitations of his claims in this chart....”

## CLAIM CHART FOR GOOGLE PRODUCTS

The following Claim Chart is an illustration of literal infringement. At least one of the alleged infringing products of Google (i.e., Google Pixel smartphones 4a, 4a(5G), 5, 6, 6a, 7, & 7a) are representative of all the alleged infringing products of Google asserted in this complaint. At least one of the alleged infringing products of Google (Google Pixel 5) is illustrated to show how the Google Pixel 5 allegedly infringes on at least one of the asserted independent claims of each of the patents-in-suit ('287, '439, and '189 patents).

Google Pixel 5 Smartphone	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
	A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;

<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	<p>X</p>	<p>X</p>
<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	<p>X</p>	<p>X</p>
<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	<p>X</p>	<p>X</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one global positioning system (GPS) connection in communication with the at least one CPU;</p>	<p>at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;</p>



<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;</p>	<p>wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;</p>	<p>at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;</p>	<p>X</p>
<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	<p>X</p>

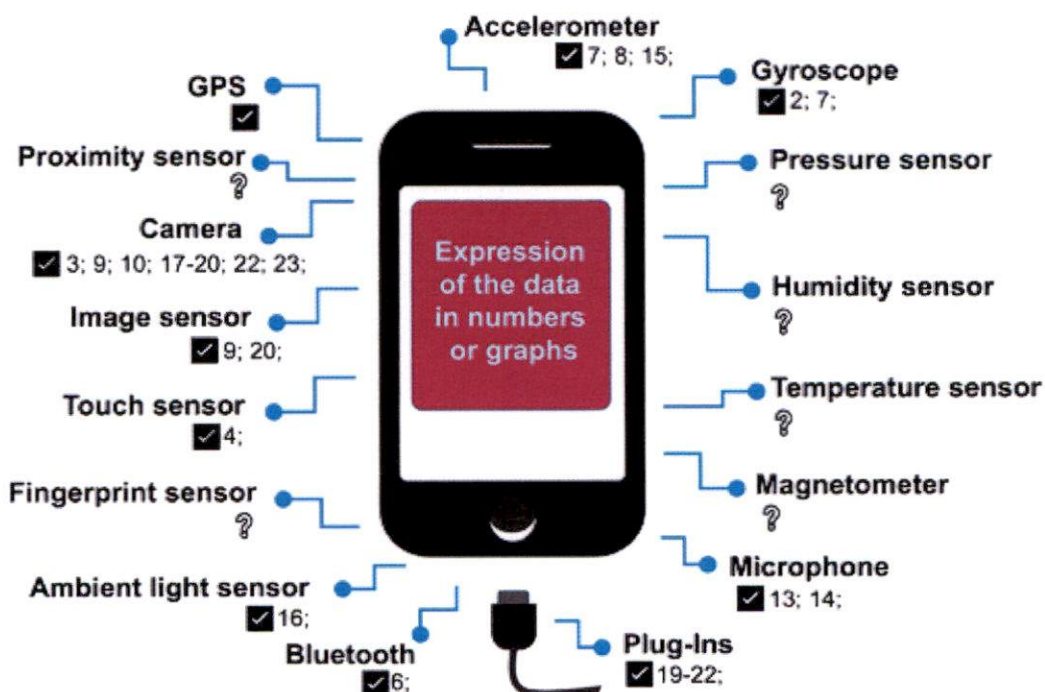
Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X
<p><b>BIOMETRICS:</b></p> <p>Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use
<p><i>Android Team Awareness Kit</i>, <i>ATAK</i> (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;	the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and	the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	X	X	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.</p>	X
--	---	--	---

### DoD DTRA ATAK Smartphone Port for CBRN Plug-Ins



Google Android and Apple iOS are “Native” to the OEMs (i.e., Google, Samsung, LG, Qualcomm, and Apple) manufacture of the smartphones.

### Blueforce Plugin Series: CBRNE and HAZMAT Response

The DuraForce Ultra 5G  
(CBRN purpose-built *plugins* for smartphones)



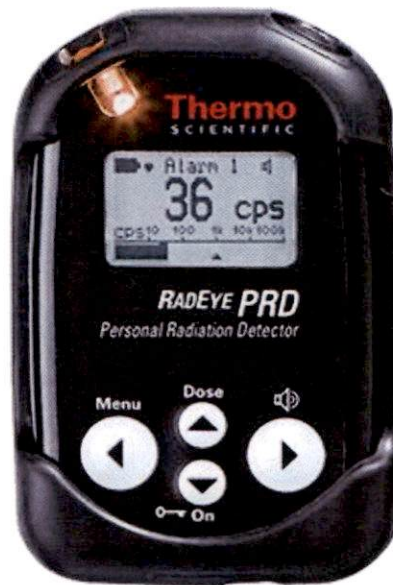
The ALTAIR 5X Gas Detector  
(Google Android and Apple iOS)



The MSA Altair 4XR Multi-Gas Detector  
(Google Android and Apple iOS)



The Thermo RadEye™ PRD Radiation Detector  
(Google Android only)



# Exhibit B



## DoD DTRA ATAK Multi-Sensor Detection System—CBRN

DoD/DTRA ATAK CBRN Sensors for the Google Pixel 5 Smartphone	Patent #: 9,589,439; Independent Claim 19	Patent #: 9,096,189; Independent Claim 7
 <p>With DTRA ... ATAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, radiological agent, or compound, comprising:</p>	<p>A multi-sensor detection system for detecting at least one explosive, nuclear, contraband, chemical, biological, human, or radiological agents and compounds, comprising:</p>
<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) With DTRA ... ATAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p> <p>The Defense Threat Reduction Agency (DTRA) CBRN ISA: Seamlessly integrates information and control of multiple sensors into a single dashboard, making it easier to detect CBRN threats and monitor a warfighter's vitals <a href="https://thelastmile.gotennapro.com/four-useful-atak-app-plugins/">https://thelastmile.gotennapro.com/four-useful-atak-app-plugins/</a></p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human, or contraband agent or compound, capable of being disposed within, on, upon or adjacent a multi-sensor detection device;</p>	<p>a plurality of sensors for detecting at least one chemical, biological, radiological, explosive, nuclear, human or contraband agents and compounds and capable of being disposed within, on, upon or adjacent a multi sensor detection device;</p>
<p>ATAK (including CivTAK) is an Android smartphone [i.e., Google smartphone] geospatial infrastructure and situational awareness app <a href="https://www.civtak.org/atak-about/">https://www.civtak.org/atak-about/</a>. ATAK can be downloaded to a phone, tablet, or handheld device. ATAK is a government-off-the-shelf app for Android smartphones. The mobile broadband 4G LTE connection is able to facilitate the data throughput required for the operation of the ATAK. <a href="https://apps.dtic.mil/sti/pdfs/AD1069441.pdf">https://apps.dtic.mil/sti/pdfs/AD1069441.pdf</a></p>	<p>monitoring equipment comprising at least one of a computer, personal computer (PC), laptop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone for at least one of a receipt or transmission of signals therebetween;</p>	<p>monitoring equipment comprising at least one of plurality product groups based on the categories of a computer, laptop, notebook, PC, handheld, cell phone, PDA or smart phone for the receipt and transmission of signals therebetween;</p>



<p>The Google phone connects to a cell tower or base station via radio waves, and that tower is usually physically connected to the infrastructure to send that data wherever it needs to go. Draper designed a chemical, biological, radiological and nuclear (CBRN) Plugin to enable users to integrate CBRN sensors into TAK, collect CBRN sensor data, display it on a map and livestream it across the TAK network to other users. CBRN plugins for ATAK, WinTAK and WebTAK are operational in the field. <a href="https://www.draper.com/explore-solutions/tak">https://www.draper.com/explore-solutions/tak</a></p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>	<p>at least one cell phone tower interconnected to the monitoring equipment for sending signals thereto and receiving signals therefrom or at least one satellite capable of transmitting signals to the monitoring equipment;</p>
<p>The Android-based [Google] smartphone[s] now contained integrated satellite on-the move capability, on-the-move mapping solutions, and a commercial laser range finder that significantly expanded the end-user range data flow and functionality. The Primary, Alternate, Contingency, and Emergency (PACE) communications architectures established was: • Primary communications structure (P): ATAK—4G/LTE; Antenna: international [] satellite (INMARSAT) <a href="https://apps.dtic.mil/sti/pdfs/AD1069441.pdf">https://apps.dtic.mil/sti/pdfs/AD1069441.pdf</a></p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;</p>	<p>at least one satellite or at least one cell phone tower capable of signal communication between the multi-sensor detection device and the monitoring equipment;</p>
<p>The internet connection is shared by many ATAK functions on the Google Pixel 5 smartphone such as internet browsing, receiving email messages and installing apps. Wi-Fi is a method for devices such as the Google Pixel 5 smartphone to connect wirelessly to the Internet using radio waves.</p>	<p>at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment;</p>	<p>at least one internet connection capable of communication between the multi-sensor detection device and the monitoring equipment;</p>

<p>Sit(x) is a commercial Server-as-a-Service solution based on the TAK platform developed by PAR Government for the U.S. Defense &amp; Intelligence Community. Sit(x) has real-time communication and information sharing. With Sit(x), individuals and teams can communicate via personal computers and handheld mobile [Google smartphone] devices by voice or text. They can share real-time full-motion video (FMV), airborne/drone imagery, GPS locations, photos, and satellite imagery. Fully secure and compatible with ATAK, WinTAK, and iTAK. Sit(x) accessed via free downloadable gateway apps.</p>	<p>whereupon a signal sent to a receiver of the multi-sensor detection device from a satellite; or to a cell phone tower; or through at least one of a short-range radio frequency or a long-range radio frequency; causes a signal to be sent to the monitoring equipment that includes at least one of location data or sensor data;</p>	<p>whereupon a signal sent to a receiver of the multi sensor detection device from a satellite; or to a cell phone tower; or through short and/or long-range radio frequency; causes a signal to be sent to the monitoring equipment that includes location data and sensor data;</p>
<p>The '439 &amp; '189 patent specs: Product grouping (PG) 1 (storage &amp; transportation); PG 2 (sensors); PG 3 (detector case; modified and adapted); PG 4 (monitoring &amp; communication devices); PG 5 (communication methods); PG 6 (biometrics); and, PG 7 (authorized person)</p>	<p>wherein the monitoring equipment or multi-sensor detection device receives a signal via any of one or more products of any product grouping categories;</p>	<p>wherein the monitoring equipment or multi sensor detection device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>The Android-based [Google] smartphone[s] now contained integrated satellite ...</p> <p>Wi-Fi is a method for devices such as the Google Pixel 5 smartphone to connect wirelessly to the Internet using radio waves...</p> <p>The internet connection is shared by many ATAK functions on the Google Pixel 5 smartphone such as internet browsing, receiving email messages; installing apps...</p> <p>The Google phone connects to a cell tower or base station via radio waves, and that tower is usually physically connected to the infrastructure to send that data wherever it needs to go.</p>	<p>wherein at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency connection, or short-range radio frequency (RF) connection is capable of signal communication with the transmitter, a receiver of the monitoring equipment, the multi-sensor detection device, or transceivers of the products;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the monitoring equipment or multi sensor detection device and transceivers of the products;</p>

<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p> <p>ATAK (including CivTAK) is an Android smartphone [i.e., Google smartphone] geospatial infrastructure and situational awareness app <a href="https://www.civtak.org/atak-about/">https://www.civtak.org/atak-about/</a>. ATAK can be downloaded to a phone, tablet, or handheld device.</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan or signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>	<p>wherein the monitoring equipment is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the monitoring device that is at least one of the computer, the laptop, the notebook, the PC, the handheld, the cell phone, the PDA, or the smart phone is locked by the biometric lock disabler to prevent unauthorized use;</p>
<p>The Android-based [Google] smartphone[s] now contained integrated satellite ...</p> <p>Wi-Fi is a method for devices such as the Google Pixel 5 smartphone to connect wirelessly to the Internet using radio waves...</p> <p>The internet connection is shared by many ATAK functions on the Google Pixel 5 smartphone such as internet browsing, receiving email messages; installing apps...</p> <p>The Google phone connects to a cell tower or base station via radio waves, and that tower is usually physically connected to the infrastructure to send that data wherever it needs to go.</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, long range radio frequency, and short-range radio frequency (RF).</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group consisting of satellite, Bluetooth, WiFi, internet, radio frequency (RF), cellular, broadband, and long and short-range radio frequency (RF).</p>

# Exhibit C

## INCLUDED IN FEDERAL CIRCUIT INFORMAL BRIEF IN GOLDEN v GOOGLE

- ❖ **BIOMETRICS:** Biometric factors allow for secure authentication on the *Android platform*. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).
- ❖ **DISABLING LOCK MECHANISM:** *Google's Android operating system* features a lock mechanism to secure your phone, known as pattern lock. When setting the pattern, you must drag your finger along lines on the screen between different nodes. Afterward, to unlock the phone, you'll need to replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. If you can't log in, you'll have to employ some other methods to restore control of your phone.
- ❖ **CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) DETECTION:** Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the *Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK)*. ATAK is a digital application available to warfighters throughout the DoD. Built on the *Android operating system*, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.
- ❖ **HEART RATE:** *Android Team Awareness Kit, ATAK* provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.
- ❖ **NEAR FIELD COMMUNICATION (NFC):** Pixel™, Phone by Google - Turn NFC on/off. *Near Field Communication (NFC)* allows the transfer of data between devices that are a few centimeters apart, typically back-to-back. NFC must be turned on for NFC-based apps (e.g., Tap to Pay) to function correctly. NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices. Tags can range in complexity.
- ❖ **WARFIGHTERS:** The U.S. armed forces and their interagency and coalition partners value *Android Team Awareness Kit, ATAK* and the common operating picture it provides. DTRA continues to develop *CBRN-specific plug-in capabilities* to support warfighters on the battlefield.

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
				
<p><b>Chipset:</b> Qualcomm Snapdragon 765G</p> <p><b>CPU:</b> Octa-core (1 × 2.4 GHz Kryo 475 Prime &amp; 1 × 2.2 GHz Kryo 475 Gold &amp; 6 × 1.8 GHz Kryo 475 Silver)</p> <p><b>OS:</b> Google Android 11, upgradable to Android 13.</p> <p><b>Modem:</b> Snapdragon® X52 5G Modem-RF System.</p>	<p><b>Chipset:</b> Apple A14 Bionic (5 nm).</p> <p><b>CPU:</b> Hexa-core (2x3.1 GHz Firestorm + 4x1.8 GHz Icestorm). <b>OS:</b> iOS 14.1, upgradable to iOS 16.1 <b>Modem:</b> Qualcomm's Snapdragon X55 5G modem</p>	<p><b>Chipset:</b> Qualcomm SM8350 Snapdragon 888 5G (5 nm). <b>CPU:</b> Octa-core (1x2.84 GHz Cortex-X1 &amp; 3x2.42 GHz Cortex-A78 &amp; 4x1.80 GHz Cortex-A55) - USA/China. <b>OS:</b> Google Android 11, upgradable to Android 13</p> <p><b>Modem:</b> Snapdragon® X60 5G Modem-RF System.</p>	<p><b>Chipset:</b> Qualcomm SM8250 Snapdragon 865 5G (7 nm+). <b>CPU:</b> Octa-core (1x2.84 GHz Cortex-A77 &amp; 3x2.42 GHz Cortex-A77 &amp; 4x1.80 GHz Cortex-A55). <b>OS:</b> Google Android 10, upgradable to Android 13</p> <p><b>Modem:</b> Qualcomm's Snapdragon X55 5G modem</p>	<p><b>Chipset:</b> Qualcomm SM8350 Snapdragon 888 5G (5 nm) <b>CPU:</b> Octa-core (1x2.84 GHz Cortex-X1 &amp; 3x2.42 GHz Cortex-A78 &amp; 4x1.80 GHz Cortex-A55). <b>OS:</b> Google Android 11.</p> <p><b>Modem:</b> Snapdragon® X60 5G Modem-RF System.</p>
<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>Temperature sensors located within; the sensors monitor the battery and processor's temperature. In extreme temperatures (hot or cold), these sensors shut down the device to prevent damage</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>

Gravity sensor supported by the Android platform. Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Accelerometer (gravity sensor) supported by the iOS platform. Accelerometer/ Motion sensor: This sensor helps the screen automatically switch from landscape to portrait modes and back again based on whether you're holding the phone vertically or horizontally.	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Gravity sensor supported by the Android platform. Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	Adjusts the screen brightness for current light conditions using the built-in ambient light sensor. Screen: 6.1" Super Retina XDR (OLED). Lock the screen orientation so that it doesn't change when the iPhone is rotated.	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.2 inches flexible OLED display at 421 ppi	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.8 inches, 109.8 cm <sup>2</sup> OLED display at 395 ppi density	Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.78 inches, 109.5 cm <sup>2</sup> OLED display at 395 ppi density
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE, NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM)</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE, NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM)</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>
<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Apple's iOS operating system features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable).</p> <p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID or enter a passcode.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>



<p>Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.</p>	<p>USB-A to Lightning cable or the newer USB-C to Lightning cable with your iPhone. The MagSafe Battery Pack makes on-the-go, wireless charging easy and reliable—just attach it to your iPhone</p>	<p>Samsung USB-C Cable lets you charge your USB-C device as well as sync your data to your smartphone</p>	<p>UrbanX USB-C to USB 3.1 Adapter, USB-C Male to USB-A Female, Uses USB OTG Technology, Compatible with LG V60 ThinQ 5G</p>	<p>ASUS / Qualcomm Smartphone for Snapdragon Insiders Dual Port 32GB USB Type C Memory Stick; 32GB USB Type-C flash drive; Features USB Type-C connector and a traditional USB connector.</p>
<p><b>BIOMETRICS:</b> Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>Apple's iOS operating system allows for Face ID authentication with the iPhone 12. The phone also features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable).</p> <p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID, Touch ID, or enter a passcode.</p>	<p><b>BIOMETRICS:</b> Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p><b>BIOMETRICS:</b> Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p><b>BIOMETRICS:</b> Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual- band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual- band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano- SIM</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/ 6e, dual-band, Wi- Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID, or enter a passcode.</p> <p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID-Touch ID or enter a passcode.</p> <p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>
<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>

<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>iOS Team Awareness Kit, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>	<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</i></p>
--	--	--	--	--

**Figure 1**

### Google's "use" of Plaintiff's Patented Central Processing Units (CPUs)

"[T]he Accused Products (i.e., Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones), which are "computers" (i.e., cell phones, computer tablets, and laptops), include components of a memory, a display, and a *processor*" ... "[w]hen in use, the "Find My Device" pre-loaded onto the Accused Product uses a *processor*" ... "[t]he "Find My Device" feature displays [] information through a *processor* using data stored in the device's memory" ... "[t]he LG Support Page lays out in a step-by-step process how to correctly remotely log in to the *processor* to access [] lock the device" ... See *Carolyn Hafeman v. LG Electronics Inc.*

In the above claim chart, the Google, Samsung, LG, and Asus/Qualcomm smartphones have Qualcomm Snapdragon Chipsets; have Octa-core CPUs (*processors*); have Google Android Operating Systems; have Qualcomm Snapdragon Modems; have Google "Find My Device" pre-installed See *Carolyn Hafeman v. LG Electronics Inc.*; have Google Android Team Awareness Kits; have Megapixel cameras for CBR sensing; have cameras for captioning nanopores; Biosensors for CBRNE detection; and, Plug-Ins for CBRN detection.



**Figure 2** is a comparative chart of the “megapixel” smartphone cameras used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK.

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Samsung Galaxy S21 Smartphone	LG V60 ThinQ 5G	Asus / Qualcomm Smartphone for Snapdragon Insiders
<p><b>Google Pixel 5:</b> Dual - 12.2 MP (megapixel), OIS 16 MP (megapixel)</p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <b>megapixel</b> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <b>pixel</b> resolution phone camera. <b>Megapixel</b> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i> Source: <a href="https://www.understandingnano.com/cell-phone-sensors-toxins.html">https://www.understandingnano.com/cell-phone-sensors-toxins.html</a></p>	<p><b>Apple iPhone 12:</b> Dual - 12 MP (megapixel), OIS 12 MP (megapixel)</p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <b>megapixel</b> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <b>pixel</b> resolution phone camera. <b>Megapixel</b> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i> Source: <a href="https://www.understandingnano.com/cell-phone-sensors-toxins.html">https://www.understandingnano.com/cell-phone-sensors-toxins.html</a></p>	<p><b>Samsung Galaxy S21:</b> Triple - 12 MP (megapixel), OIS 64 MP (megapixel)</p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <b>megapixel</b> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <b>pixel</b> resolution phone camera. <b>Megapixel</b> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i> Source: <a href="https://www.understandingnano.com/cell-phone-sensors-toxins.html">https://www.understandingnano.com/cell-phone-sensors-toxins.html</a></p>	<p><b>LG V60 ThinQ 5G:</b> Dual - 64 MP (megapixel), OIS 13 MP (megapixel)</p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <b>megapixel</b> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <b>pixel</b> resolution phone camera. <b>Megapixel</b> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i> Source: <a href="https://www.understandingnano.com/cell-phone-sensors-toxins.html">https://www.understandingnano.com/cell-phone-sensors-toxins.html</a></p>	<p><b>Asus / Qualcomm:</b> Triple - 64 MP (megapixel) OIS; 8 MP, 12MP (mega)</p> <p>Camera lens in cell phone with microfluidic lens functions as camera; uses microscope to focus on a chemical sensor. A <b>megapixel</b> camera captures the image from the array of nanopores uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the <b>pixel</b> resolution phone camera. <b>Megapixel</b> resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. <i>Tiny sensors tucked into cell phones could map airborne toxins in real time.</i> Source: <a href="https://www.understandingnano.com/cell-phone-sensors-toxins.html">https://www.understandingnano.com/cell-phone-sensors-toxins.html</a></p>

**Figure 2**



**Figure 3** is a visual display of different ways the smartphone camera <sup>1 2</sup> can be used for detecting Chem/Bio agents. For each different way used, it qualifies as an alternative to the ATAK.

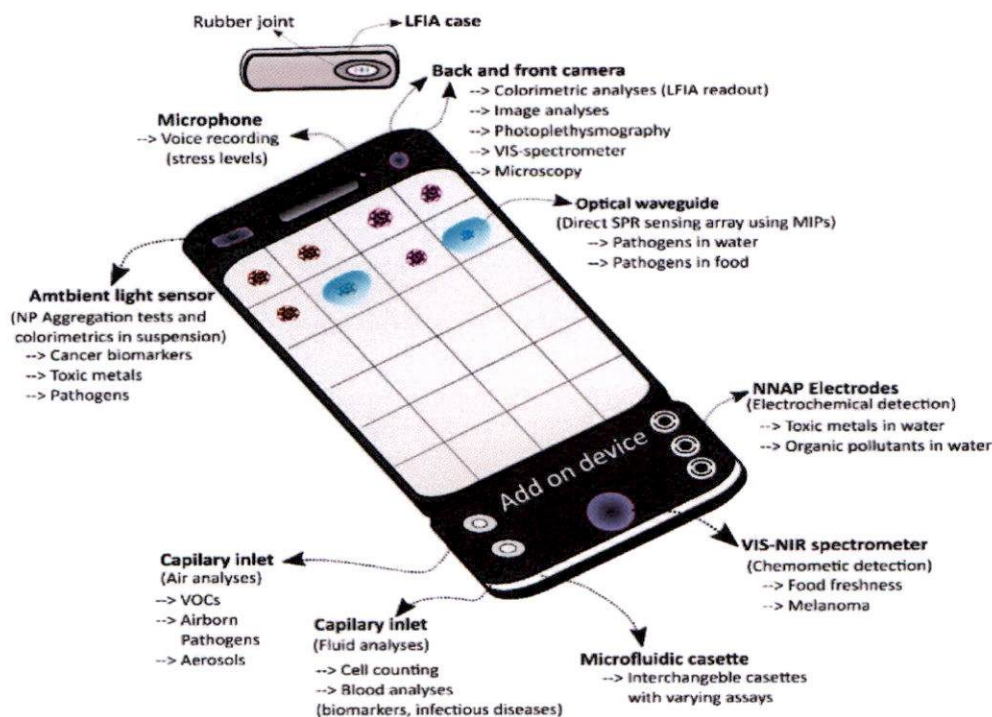


**Figure 3**

1 The camera captures the image from the array of nanopores that uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the resolution phone camera. The resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: [https:// www.understanding nano.com/cell-phone-sensors-toxins.html](https://www.understandingnano.com/cell-phone-sensors-toxins.html)

2 Hyperspectral imaging scans for light frequencies that humans can't see in order to identify the unique chemical signatures of different substances. They say their device, which can be mass produced, is compatible with all standard smartphone cameras. *These New Smartphone Cameras Could Tell You What an Object Is Made of* <https://www.sciencealert.com/new-smartphone-cameras-could-tell-you-what-an-object-is-made-of>

**Figure 4** describes how at least nine (9) standard sensors for the Google, Apple, Samsung, LG, and Asus/Qualcomm smartphones can be used as “biosensors”. For each different way used, it qualifies as an alternative to ATA.



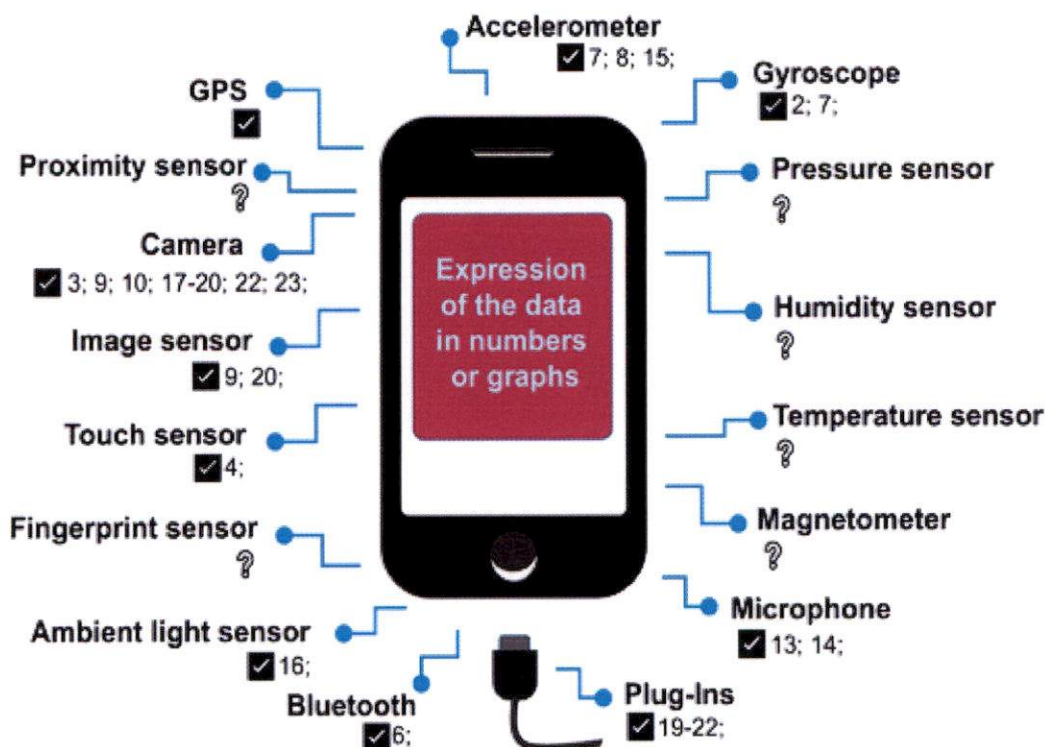
**Figure 4**

#### The Smartphones Biosensors:

1. Ambient light sensor: Cancer biomarkers; Toxic metals; Pathogens
2. Capillary inlet: (Air analysis). Airborne Pathogens; Aerosols
3. Capillary inlet: (Fluid analysis). Blood analysis; Biomarkers
4. Microfluidic cassette: Interchangeable cassettes with varying assays
5. VIS-NIR spectrometer: Food freshness; Melanoma
6. NNAP Electrodes: Toxic metals and Organic pollutants in water
7. Optical Waveguide: Pathogens in water and food
8. Back and front camera: Colorimetric analysis; Image analysis
9. Microphone: Voice recording stress levels



**Figure 5** list some of the same standard sensors illustrated in Figure 4. The port on the smartphones is used for the CBRN *plug-ins* included in ATAK.





**Figure 5**

ATAK is a digital application available to warfighters throughout the DoD. Built on the Android operating system, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) *plug-ins*.

Just having a plug-in is not all that’s involved. There has to be an app specific software to sync the chemical, biological, radiological, and nuclear sensors to the smartphone plus the Google Android Operating System.

# Exhibit D

## Google Pixel 5 Smartphone and Apple iPhone 12 Smartphone Comparison

Google Pixel 5 Smartphone	Apple iPhone 12 Smartphone	Claim 5 of the '287 Patent	Claim 23 of the '439 Patent	Claim 1 of the '189 Patent
		A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	CPU: Hexa-core (2x3.1 GHz Firestorm + 4x1.8 GHz Icestorm). System-on-a-chip: Apple A14 Bionic (5 nm). iOS 14.1, upgradable to iOS 16.1	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;
Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.	Temperature sensors located within; the sensors monitor the battery and processor's temperature. In extreme temperatures (hot or cold), these sensors shut down the device to prevent damage	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X

Gravity sensor supported by the Android platform. Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	Accelerometer (gravity sensor) supported by the iOS platform. Accelerometer/Motion sensor: This sensor helps the screen automatically switch from landscape to portrait modes and back again based on whether you're holding the phone vertically or horizontally.	at least one motion sensor in communication with the at least one CPU;	X	X
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	Adjusts the screen brightness for current light conditions using the built-in ambient light sensor. Screen: 6.1" Super Retina XDR (OLED). Lock the screen orientation so that it doesn't change when the iPhone is rotated.	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual-band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano-SIM; eSIM or Dual SIM	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual- band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano- SIM; eSIM or Dual SIM</p>	<p>at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;</p>	<p>wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual- band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano- SIM; eSIM or Dual SIM</p>	<p>at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;</p>	<p>at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;</p>	<p>X</p>
<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest x Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Apple's iOS operating system features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable).</p> <p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID or enter a passcode.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi- sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	<p>X</p>

Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.	USB-A to Lightning cable or the newer USB-C to Lightning cable with your iPhone. The MagSafe Battery Pack makes on-the-go, wireless charging easy and reliable—just attach it to your iPhone	at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;	X	X
BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).	<p>Apple's iOS operating system allows for Face ID authentication with the iPhone 12. The phone also features a lock mechanism to secure your phone. After multiple failed attempts to unlock the phone, the phone locks and is disabled (made unavailable).</p> <p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID, Touch ID, or enter a passcode.</p>	at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;	wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and	wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 5 802.11 a/b/g/n/ac/6, dual- band, hotspot. Bluetooth 5.0. NFC, GPS, GLONASS, Galileo, QZSS Nano- SIM; eSIM or Dual SIM</p>	<p>at least one radio- frequency near- field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID, or enter a passcode.</p> <p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies</p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>



<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, iATAK</i> (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>Apple Home Key digital security code is stored in Apple Wallet app. It is based on NFC technology. 2 modes of operation: Express Mode: Bring an iPhone or Apple Watch to the lock. Face ID or Passcode. Must use Face ID / Touch ID or enter a passcode.</p> <p><i>iOS Team Awareness Kit, iTAK</i> (built on the iOS 14.1, or later, operating system) provides an interface for viewing and controlling different CBRN-sensing technologies</p>	X	X	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>
<p><i>Android Team Awareness Kit, iATAK</i> (built on the Android operating system) is a digital application available to warfighters throughout the DoD. iATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>iOS Team Awareness Kit, iTAK</i> (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>iOS Team Awareness Kit</i>, iTAK (built on the iOS 14.1, or later, operating system) is a digital application available to warfighters throughout the DHS / DoD. iTAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, iTAK includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>X</p>	<p>whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.</p>	<p>X</p>
--	--	----------	--	----------

**Figure 1** outline different ways the smartphone camera can be used for detecting Chem/Bio agents. For each different way used it qualifies as an alternative to the Google Android ATAK and Apple iOS iTAK.

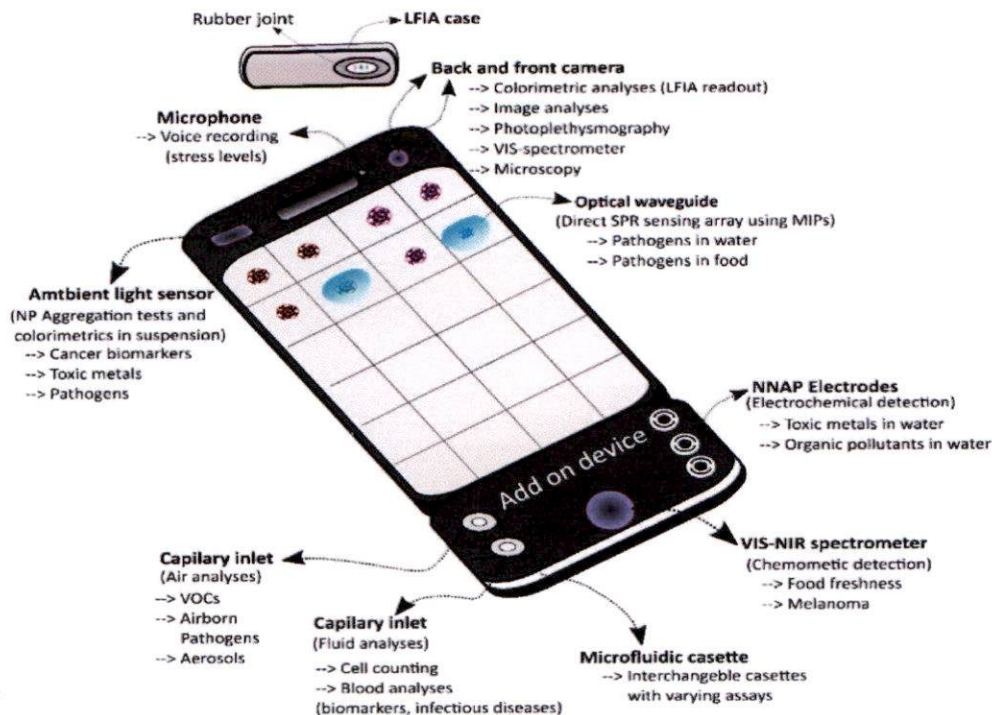


**Figure 1**

The camera captures the image from the array of nanopores that uses fluid rather than bulky moving parts. The sensors contained in one array is determined by the resolution phone camera. The resolution in cell phone cameras; probe a million different spots on the sensor simultaneously. *Tiny sensors tucked into cell phones could map airborne toxins in real time.* Source: [https:// www.understanding nano.com/cell-phone-sensors-toxins.html](https://www.understandingnano.com/cell-phone-sensors-toxins.html)

Hyperspectral imaging scans for light frequencies that humans can't see in order to identify the unique chemical signatures of different substances. They say their device, which can be mass produced, is compatible with all standard smartphone cameras. *These New Smartphone Cameras Could Tell You What an Object Is Made of* <https://www.sciencealert.com/new-smartphone-cameras-could-tell-you-what-an-object-is-made-of>

**Figure 2** describes how at least nine (9) standard “Native” sensors for the smartphone can be used as “biosensors”. For each different way used it qualifies as an alternative to the Google Android ATAK and Apple iOS iTAK.



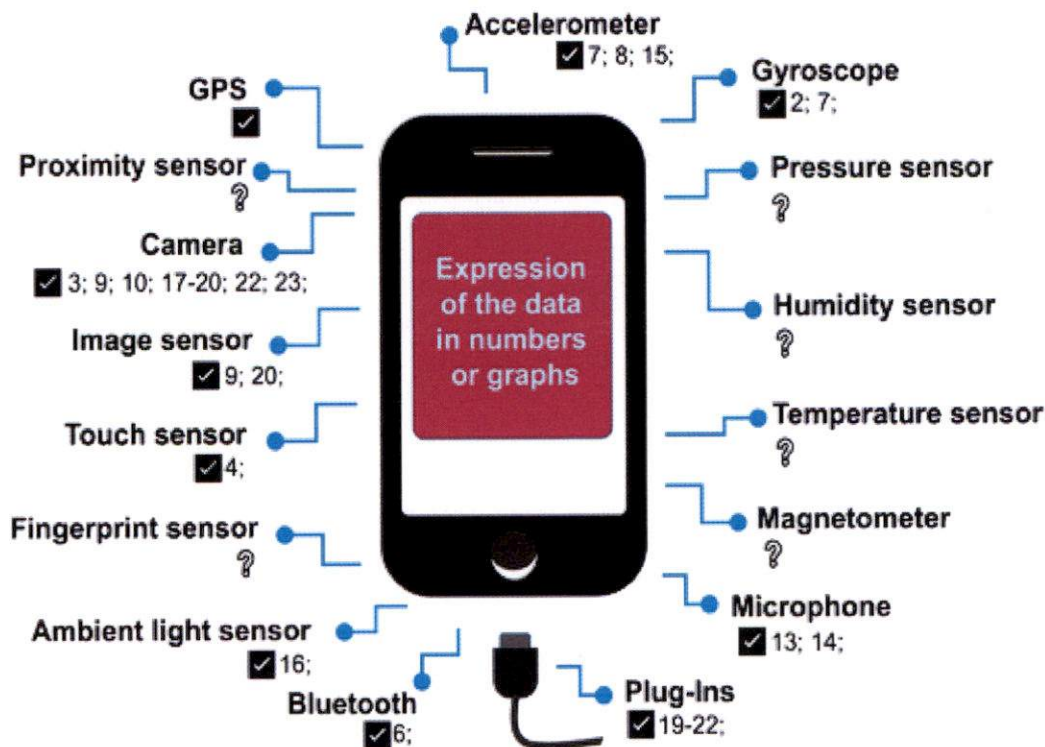
**Figure 2**

The Smartphones Biosensors:

1. Ambient light sensor: Cancer biomarkers; Toxic metals; Pathogens
2. Capillary inlet: (Air analysis). Airborne Pathogens; Aerosols
3. Capillary inlet: (Fluid analysis). Blood analysis; Biomarkers
4. Microfluidic cassette: Interchangeable cassettes with varying assays
5. VIS-NIR spectrometer: Food freshness; Melanoma
6. NNAP Electrodes: Toxic metals and Organic pollutants in water
7. Optical Waveguide: Pathogens in water and food
8. Back and front camera: Colorimetric analysis; Image analysis
9. Microphone: Voice recording stress levels



**Figure 3** “Native” to the smartphone is a “port” for *plug-ins* that are at least: embedded into, affixed to, placed upon; software based, or hardware based, wired or wireless connection, for CBRNE detection.



**Figure 3**

### **Blueforce Plugin Series: CBRNE and HAZMAT Response (See also *Figure 8*)**

BlueforceTACTICAL (CBRN purpose-built *plugins* for smartphones): The DuraForce Ultra 5G is Kyocera’s toughest, most durable smartphone to date, certified to military standard 810H (MIL-STD-810H) to withstand drops



BlueforceTACTICAL (Google Android and Apple iOS): The ALTAIR 5X Gas Detector is capable of measuring up to 6 gases simultaneously and is now available with integrated PID sensor for VOC detection. The 5X provide real-time environmental awareness when paired via Bluetooth® with the BlueforceTACTICAL MSA *Plugin*.

BlueforceTACTICAL (Google Android and Apple iOS): The MSA Altair 4XR Multi-Gas Detector detects O<sub>2</sub>, LEL, CO and H<sub>2</sub>S. Outfitted with rapid-response MSA XCell® sensors, the ALTAIR 4XR Gas Detector is the toughest 4-gas monitor on the market and is backed by a 4-year warranty. The ALTAIR 4XR can also provide real-time incident awareness when paired via Bluetooth® with the BlueforceTACTICAL MSA *Plugin*.

BlueforceTACTICAL (Google Android only): Detect and localize radiation sources generated by manmade devices such as nuclear weapons, improvised nuclear devices (INDs) or radiological dispersal devices (RDDs) with the Thermo Scientific™ RadEye™ PRD Personal Radiation Detector. The BlueforceTACTICAL *Plugin* shares PRD data with other responders and can simultaneously push readings to cloud databases for longitudinal analysis.

# Exhibit E

**CLAIM CHART FOR THE SMARTPHONE COMPARISON BETWEEN  
THE GOOGLE PIXEL 5 AND THE SAMSUNG GALAXY S21. THE  
GOOGLE PIXEL 5 SPECIFICATIONS AND THE PATENT CLAIMS'  
LIMITATIONS FOR THE '287, '439, & '189 PATENTS ARE THE SAME  
AS IN *LARRY GOLDEN v. GOOGLE LLC*; CAFC CASE NO. 22-1267**

Google Pixel 5 Smartphone	Samsung Galaxy S21 Smartphone	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
		<p>A monitoring device, comprising:</p>	<p>A cell phone comprising:</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>
<p>CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime &amp; 1 × 2.2 GHz Kryo 475 Gold &amp; 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G</p>	<p>CPU: Octa-core (1x2.84 GHz Cortex-X1 &amp; 3x2.42 GHz Cortex-A78 &amp; 4x1.80 GHz Cortex-A55) - USA/China. Chipset: Qualcomm SM8350 Snapdragon 888 5G (5 nm). OS: Google Android 11, upgradable to Android 13 Modem: Snapdragon® X60 5G Modem-RF System.</p>	<p>at least one central processing unit (CPU);</p>	<p>a central processing unit (CPU) for executing and carrying out the instructions of a computer program;</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;</p>

<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	X	X
<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	X	X
<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi</p>	<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.2 inches flexible OLED display at 421 ppi</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	X	X



Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;	X

<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	X
<p>Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.</p>	<p>Samsung USB-C Cable lets you charge your USB-C device as well as sync your data to your smartphone</p>	<p>at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;</p>	X	X

<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;</p>	<p>wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents</p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>



<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct. Bluetooth 5.0, A2DP, LE. NFC, GPS, GLONASS, BDS, GALILEO. Nano-SIM and eSIM or Dual SIM</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>X</p>	<p>X</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.</p>	X

# Exhibit F

**CLAIM CHART FOR THE SMARTPHONE COMPARISON BETWEEN  
THE GOOGLE PIXEL 5 AND LG V60 ThinQ 5G. THE GOOGLE PIXEL 5  
SPECIFICATIONS AND THE PATENT CLAIMS' LIMITATIONS FOR  
THE '287, '439, & '189 PATENTS ARE THE SAME AS IN *LARRY  
GOLDEN v. GOOGLE LLC*; CAFC CASE NO. 22-1267**

Google Pixel 5 Smartphone	LG V60 ThinQ 5G	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
		<p>A monitoring device, comprising:</p>	<p>A cell phone comprising:</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>
<p>CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime &amp; 1 × 2.2 GHz Kryo 475 Gold &amp; 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G</p>	<p><b>Chipset:</b> Qualcomm SM8250 Snapdragon 865 5G (7 nm+). <b>CPU:</b> Octa-core (1x2.84 GHz Cortex-A77 &amp; 3x2.42 GHz Cortex-A77 &amp; 4x1.80 GHz Cortex-A55). <b>OS:</b> Google Android 10, upgradable to Android 13 <b>Modem:</b> Qualcomm's Snapdragon X55 5G modem</p>	<p>at least one central processing unit (CPU);</p>	<p>a central processing unit (CPU) for executing and carrying out the instructions of a computer program;</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;</p>



<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	<p>X</p>	<p>X</p>
<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	<p>X</p>	<p>X</p>
<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi</p>	<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.8 inches, 109.8 cm<sup>2</sup> OLED display at 395 ppi density</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	<p>X</p>	<p>X</p>

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;	X

<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	X
<p>Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.</p>	<p>UrbanX USB-C to USB 3.1 Adapter, USB-C Male to USB-A Female, Uses USB OTG Technology, Compatible with LG V60 ThinQ 5G</p>	<p>at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;</p>	X	X

<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;</p>	<p>wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents</p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, DLNA. Bluetooth 5.1, A2DP, LE, aptX HD. NFC, GPS, GPS, GLONASS, Galileo, BDS. Single SIM (Nano-SIM) or Hybrid Dual SIM (Nano-SIM, dual stand-by)</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>



<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>X</p>	<p>X</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.</p>	X

# Exhibit G



**CLAIM CHART FOR THE SMARTPHONE COMPARISON BETWEEN THE GOOGLE PIXEL 5 AND THE ASUS / QUALCOMM. THE GOOGLE PIXEL 5 SPECIFICATIONS AND THE PATENT CLAIMS' LIMITATIONS FOR THE '287, '439, & '189 PATENTS ARE THE SAME AS IN *LARRY GOLDEN v. GOOGLE LLC*; CAFC CASE NO. 22-1267**

Google Pixel 5 Smartphone	Asus / Qualcomm Smartphone for Snapdragon Insiders	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
		A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	<b>Chipset:</b> Qualcomm SM8350 Snapdragon 888 5G (5 nm) <b>CPU:</b> Octa-core (1x2.84 GHz Cortex-X1 & 3x2.42 GHz Cortex-A78 & 4x1.80 GHz Cortex-A55). <b>OS:</b> Google Android 11. <b>Modem:</b> Snapdragon® X60 5G Modem-RF System.	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;

<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.</p>	<p>Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures.</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	X	X
<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>Gravity sensor supported by the Android platform. Measures the force of gravity in m/s<sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	X	X
<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi</p>	<p>Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6.78 inches, 109.5 cm<sup>2</sup> OLED display at 395 ppi density</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	X	X

Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)	at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;	at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;	X

<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest x Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest x Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	X
<p>Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.</p>	<p>ASUS / Qualcomm Smartphone for Snapdragon Insiders Dual Port 32GB USB Type C Memory Stick; 32GB USB Type-C flash drive; Features USB Type-C connector and a traditional USB connector.</p>	<p>at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;</p>	X	X

<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>BIOMETRICS: Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;</p>	<p>wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents</p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>Connectivity: Wi-Fi 802.11 a/b/g/n/ac/6e, dual-band, Wi-Fi Dir. Bluetooth: 5.2, A2DP, LE, aptX HD, aptX Adaptive. NFC, GPS, GLONASS, BDS, Galileo, QZSS, Dual SIM (Nano-SIM, dual stand-by)</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</i></p>	<p>X</p>	<p>X</p>	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.</p>	X




# Exhibit H

## PLAINTIFF'S ILLUSTRATIVE CLAIM CHART FOR PATENT INFRINGEMENT

Below, is an illustrative claim chart of how the Samsung Galaxy Book2 Pro 360 PC / Tablet directly infringes claim 5 of Plaintiff's '287 patent, and claim 1 of Plaintiff's '189 patent.

Also, the chart illustrates how Intel® Core™ i5-1235U / Intel® Core™ i7-1255U CPU contributes to the infringement of the Samsung Galaxy Book2 Pro 360 PC / Tablet, and has “no substantial non-infringing use”. Plaintiff's CPU is referenced in 12 limitations of claim 5 of Plaintiff's '287 patent. Every claim limitation is covered.

Samsung Galaxy Book2 Pro 360 [PC Mode or Tablet Mode]	Patent #: 10,163,287; Indep. Claim 5	Patent #: 9,096,189; Independent Claim 1
 <p>This “<i>doctrine of equivalent</i>” element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p>	<p>A monitoring device, comprising:</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>
<p>CPU: Intel® Core™ i5-1235U / Intel® Core™ i7-1255U. Processor Speed 1.3GHz / 1.7 GHz. Clock 900 - 4400 MHz / 1200 - 4700 MHz. L1 Cache 928 KB / 928 KB. Cores 10 / 10. Threads 12 / 12. Preinstalled Operating System Windows 11 Home</p> <p>This “<i>doctrine of equivalent</i>” element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claims.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one central processing unit (CPU);</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;</p>

<p>Technical Specifications: CPU Temperature Sensor reached 99° C. Surface temperature: W,A,S,D Keys - 42.1 °C, Keyboard Middle - 44.1 °C, Palm Rest - 37.0 °C</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	<p>X</p>
<p>With the infrared sensor the device can detect motion by measuring the infrared (IR) light radiating from objects in its field of view</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	<p>X</p>
<p>Available in two screen sizes (13.3" and 15.6"). Plus, the screen automatically adapts to any lighting environment, so it's easy on the eyes, thanks to a 1MM:1 contrast ratio</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	<p>X</p>
<p>GPS: If you turn on satellite-based GPS, your tablet can find your exact position. Microsoft Windows 11 has added a location services feature that uses IP addresses and Wi-Fi positioning to predict your location.</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one global positioning system (GPS) connection in communication with the at least one CPU;</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;</p>

<p>High speed internet and Microsoft account required for Windows 11 Home and Windows 11 Pro. Networking: 802.11ax (Wi-Fi 6E), Bluetooth Standard: Bluetooth 5.0</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...</p>
<p>Networking: Bluetooth Standard: Bluetooth 5.0. 802.11ax (Wi-Fi 6E),</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;</p>	<p>X</p>
<p>Galaxy Book2 Pro 360 Specs: The Galaxy Book2 Pro keyboard has an NFC connection spot. Tapped the Galaxy phone on the spot to make contact; then used the Samsung Flow phone software to lock and unlock the tablet using the phone's fingerprint scanner.</p> <p>Windows Hello face authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock.</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>X</p>


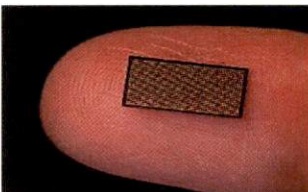
<p>Samsung's Super-Fast Charging-enabled 65W AC adapter in the box. It can deliver "8 hours" of battery life in just 30 minutes of charging. The Galaxy Book2 Pro 360 averaged around 10 hours 30 minutes on a full charge.</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> The CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360 and is capable of carrying out the functional and operational instructions of the PC.</p>	<p>at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;</p>	<p>X</p>
<p>Samsung's Biometric Sensors. Fingerprint Reader. Windows Hello face authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock.</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>
<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the Galaxy Book2 Pro 360</p> <p>This "<b>doctrine of equivalent</b>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p> <p><b>Induced infringement:</b> requires not 'only knowledge of the patent' but also 'proof the defendant knew the [induced] acts were infringing.'" <i>DSU Med. Corp. v. JMS Co.</i>, 471 F.3d 1293, 1305 (Fed. Cir. 2006) Notice to Appeal sent to Samsung in <i>Golden v. USA</i> Case 13-307C</p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>

<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the Galaxy Book2 Pro 360</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p> <p><b>Induced infringement:</b> requires not 'only knowledge of the patent' but also 'proof the defendant knew the [induced] acts were infringing.'" <i>DSU Med. Corp. v. JMS Co.</i>, 471 F.3d 1293, 1305 (Fed. Cir. 2006) Notice to Appear sent to Samsung in <i>Golden v. USA</i> Case 13-307C</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>The Galaxy Book2 Pro keyboard has a Near Field Communications (NFC) connection spot. Briefly tapped the Galaxy phone on the spot to make contact</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>
<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the Galaxy Book2 Pro 360</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p> <p><b>Induced infringement:</b> requires not 'only knowledge of the patent' but also 'proof the defendant knew the [induced] acts were infringing.'" <i>DSU Med. Corp. v. JMS Co.</i>, 471 F.3d 1293, 1305 (Fed. Cir. 2006). Notice to Appear sent to Samsung in <i>Golden v. USA</i> Case 13-307C</p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building... or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>



<p>The Galaxy Book2 Pro keyboard has a Near Field Communications (NFC) connection spot. Briefly tapped the Galaxy phone on the spot to make contact; then used the Samsung Flow phone software to lock and unlock the Galaxy Book2 Pro tablet using the phone's fingerprint scanner from across the room.</p> <p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the Galaxy Book2 Pro 360</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	X	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>
<p>High speed internet and Microsoft account required for Windows 11 Home and Windows 11 Pro. Networking: 802.11ax (Wi-Fi 6E), Bluetooth Standard: Bluetooth 5.0</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing Galaxy Book2 Pro 360</p>	X	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>

### Intel contributed to the infringement of Plaintiff's patented new and improved upon PC

<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals. Below: Intel Labs' Nabil Imam holds a Loihi neuromorphic chip in his Santa Clara, California, neuromorphic computing lab. (Walden Kirsch/Intel Corp)</p>	
<p>Intel and Cornell trained Intel's Loihi neuromorphic chip to learn and recognize the scents of 10 hazardous chemicals ... the activity of 72 chemical sensors in response to these smells and configured the circuit diagram of biological olfaction on Loihi. The chip quickly learned the neural representation of each of the smells and each odor.</p>	 <p>Intel's Loihi 2 Neuromorphic Chip</p>




# Exhibit I

## PLAINTIFF'S ILLUSTRATIVE CLAIM CHART FOR PATENT INFRINGEMENT

Below, is an illustrative claim chart of how the HP ZBook PC directly infringes claim 5 of Plaintiff's '287 patent, and claim 1 of Plaintiff's '189 patent.

Also, the chart illustrates how Intel's 11th Generation Intel® Xeon® W-11955M vPro® CPU contributes to the infringement of the HP ZBook PC, and has "no substantial non-infringing use". Plaintiff's CPU is referenced in 12 limitations of claim 5 of Plaintiff's '287 patent. Every claim limitation is covered.

HP ZBook Fury 15.6 Inch G8 Mobile Workstation PC	Patent #: 10,163,287; Indep. Claim 5	Patent #: 9,096,189; Independent Claim 1
 <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p>	<p>A monitoring device, comprising:</p>	<p>A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:</p>
<p>CPU: 11<sup>th</sup> Generation Intel® Xeon® W-11955M vPro® with Intel® UHD Graphics (2.6 GHz base frequency, up to 5.0 GHz with Intel® Turbo Boost Technology, 24 MB cache, 8 cores; 16 threads). Preinstalled operating system - Windows 11 Pro2</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claims.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one central processing unit (CPU);</p>	<p>at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;</p>

<p>Technical Specifications Temperature Sensor— Operating is 14° to 158° F (-10° to 70° C).</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one temperature sensor in communication with the at least one CPU for monitoring temperature;</p>	<p>X</p>
<p>HP CoolSense Technology uses a motion sensor to sense when the computer is being used in a stationary or mobile setting</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one motion sensor in communication with the at least one CPU;</p>	<p>X</p>
<p>15.6" diagonal UHD (3840 x 2160) IPS eDP1.4 + PSR2 WLED-backlit touch screen with Corning® Gorilla® Glass 5</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one viewing screen for monitoring in communication with the at least one CPU;</p>	<p>X</p>
<p>GPS: Standalone, A-GPS (MS-A, MS-B). GPS Bands: 1575.42 MHz ± 1.023 MHz, GLONASS 1596-1607MHz, Beidou 1561.098 MHz</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one global positioning system (GPS) connection in communication with the at least one CPU;</p>	<p>at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;</p>

<p>High speed internet and Microsoft account required for Windows 11 Pro and Windows 11 Pro for Business</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;</p>	<p>wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...</p>
<p>WLAN: Intel® Wi-Fi 6 AX201 (2x2) and Bluetooth® 5.2 wireless card, vPro™</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;</p>	<p>X</p>
<p>HP ZBook PC Specs: HP Tamper Lock. Nano Security Lock. Windows Hello face authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock.</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>X</p>


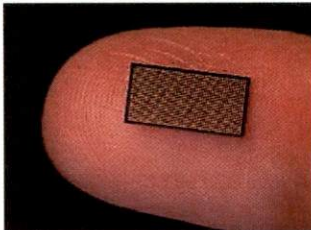
<p>HP chipset requires a Windows operating system, network hardware and software, connection with a power source, and a direct corporate network connection which is either cable or wireless LAN.</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> The CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC and is capable of carrying out the functional and operational instructions of the PC.</p>	<p>at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;</p>	<p>X</p>
<p>HP Fingerprint Sensor. Windows Hello face authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock.</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>
<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the HP ZBook PC</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p> <p><b>Induced infringement:</b> requires not 'only knowledge of the patent' but also 'proof the defendant knew the [induced] acts were infringing.'" <i>DSU Med. Corp. v. JMS Co.</i>, 471 F.3d 1293, 1305 (Fed. Cir. 2006)</p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>

<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the HP ZBook PC</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p> <p><b>Induced infringement:</b> requires not 'only knowledge of the patent' but also 'proof the defendant knew the [induced] acts were infringing.'" <i>DSU Med. Corp. v. JMS Co.</i>, 471 F.3d 1293, 1305 (Fed. Cir. 2006)</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Near Field Communication (NFC) module. NFC RF standards ISO/IEC 14443 A</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>
<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the HP ZBook PC</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p> <p><b>Induced infringement:</b> requires not 'only knowledge of the patent' but also 'proof the defendant knew the [induced] acts were infringing.'" <i>DSU Med. Corp. v. JMS Co.</i>, 471 F.3d 1293, 1305 (Fed. Cir. 2006)</p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building... or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>



<p>HP ZBook PC Specs: HP Tamper Lock. Nano Security Lock.</p> <p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals compatible with the HP ZBook PC</p> <p>This "<i>doctrine of equivalent</i>" element performs substantially the same function; in substantially the same way; and, produces substantially the same result, as the element as expressed in the claim.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	X	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>
<p>High speed internet and Microsoft account required for Windows 11 Pro and Windows 11 Pro for Business. WLAN: Intel® Wi-Fi 6 AX201 (2x2) and Bluetooth® 5.2 wireless card, vPro™</p> <p><b>Literal Infringement:</b> When there is a direct correspondence between the words in the patent claims and the infringing product or device or technology.</p> <p><b>Contributory infringement:</b> This CPU element, provided by Intel, is a material component of the allegedly infringing HP ZBook PC</p>	X	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>

### Intel contributed to the infringement of Plaintiff's patented new and improved upon PC

<p>Intel's Loihi Neuromorphic Chip to Learn and Recognize the Scents of 10 Hazardous Chemicals. Below: Intel Labs' Nabil Imam holds a Loihi neuromorphic chip in his Santa Clara, California, neuromorphic computing lab. (Walden Kirsch/Intel Corp)</p>	
<p>Intel and Cornell trained Intel's Loihi neuromorphic chip to learn and recognize the scents of 10 hazardous chemicals ... the activity of 72 chemical sensors in response to these smells and configured the circuit diagram of biological olfaction on Loihi. The chip quickly learned the neural representation of each of the smells and each odor, demonstrating a future for neuroscience and AI.</p>	 <p>Intel's Loihi 2 Neuromorphic Chip</p>

Sincerely,

s/ Larry Golden

Larry Golden, *Pro Se* Plaintiff

740 Woodruff Rd., #1102

Greenville, SC 29607

(H) 8642885605

(M) 8649927104

Email: atpg-tech@charter.net



**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that on this 19<sup>th</sup> day of June, 2023, a true and correct copy of the foregoing “Plaintiff’s Motion for Summary Judgement”, was served upon the following Defendant via email and by priority “express” mail:

Grant D. Johnson  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
Grant.D.Johnson@usdoj.gov  
(202) 305-2513

s/ Larry Golden

Larry Golden, Pro Se  
740 Woodruff Rd., #1102  
Greenville, South Carolina 29607  
atpg-tech@charter.net  
864-288-5605

# *Exhibit*

3

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN,

Plaintiff, *pro se*,

v.

THE UNITED STATES,

Defendant.

No. 13-307 C

Senior Judge Eric G. Bruggink

**DEFENDANT UNITED STATES' MOTION FOR NOTICE**

The United States of America ("the Government") moves for the Court to issue notice pursuant to Rule 14(b) of the Rules of the Court of Federal Claims ("RCFC") that pursuant to Rule 14(c), if they so desire, the following entities may appear and defend any interests that they may have:

1. The Boeing Company  
c/o Corporation Service  
Company  
251 Little Falls Drive  
Wilmington, DE 19808  
(302) 636-5401
2. Lockheed Martin Corporation  
c/o Corporation Service  
Company  
251 Little Falls Drive  
Wilmington, DE 19808  
(302) 636-5401
3. Northrop Grumman  
Corporation  
c/o Corporation Trust  
Company  
Corporation Trust Center  
1209 Orange St.  
Wilmington, DE 19801  
(302) 658-7581
4. Oshkosh Corporation  
c/o CT Corporation System  
301 S. Bedford Street  
Suite 1  
Madison, WI 53703-3691
5. Raytheon Company  
c/o Corporation Trust  
Company  
Corporation Trust Center  
1209 Orange St.  
Wilmington, DE 19801  
(302) 658-7581
6. Kratos Defense & Security  
Solutions, Inc.  
c/o Corporation Service  
Company  
251 Little Falls Drive  
Wilmington, DE 19808  
(302) 636-5401

Received - USCFC

MAR 18 2019

- |   |  |
|---|--|
| <p>7. Qualcomm Inc.<br/>c/o The Prentice-Hall<br/>Corporation System, Inc.<br/>251 Little Falls Drive<br/>Wilmington, DE 19808<br/>(302) 636-5400</p>                               | <p>9. iControl, Inc.<br/>c/o Corporation Service<br/>Company<br/>251 Little Falls Drive<br/>Wilmington, DE 19808<br/>(302) 636-5401</p>  |
| <p>8. Integrated Device<br/>Technology, Inc.<br/>c/o Corporation Trust<br/>Company<br/>Corporation Trust Center<br/>1209 Orange St.<br/>Wilmington, DE 19801<br/>(302) 658-7581</p> | <p>10. Eureka Aerospace, Inc.<br/>c/o Dr. James Tatoian<br/>3800 Shadow Grove Rd.<br/>Pasadena, CA 91107</p> <p>11. DreamHammer Inc.<br/>c/o Nelson Paez<br/>11835 W. Olympic<br/>Boulevard<br/>Suite 285E<br/>Los Angeles, CA 90064</p> |

Although the Government was under no obligation to do so, on March 15, 2019, the Government inquired via e-mail whether or not Plaintiff would oppose the Government's Motion For Notice so that the Government could indicate Plaintiff's position in this Motion. On March 17, 2019, Plaintiff responded simply with "Yes." Accordingly, although the Government does not believe Plaintiff has sufficient grounds to oppose notifying the above-identified third parties of this litigation, Plaintiff's response suggests that he will oppose on some basis.

#### STATEMENT IN SUPPORT OF MOTION

Plaintiff's Final Complaint (Dkt. 120) alleges infringement of numerous patents under 28 U.S.C. § 1498(a) by dozens of projects allegedly involving the Government. After the majority of these allegations were dismissed (Dkt. 130), the Court provided Plaintiff with an opportunity to voluntarily dismiss any remaining patent infringement allegations pursuant to RCFC 41. Dkt. 151 at 4. To date, however, Plaintiff does not appear to have filed such a voluntary

dismissal. Accordingly, the case is proceeding on the various patent infringement claims that remain. *See id.*

The chart below lists the eleven (11) products/projects that are accused of infringing Plaintiff's various patents. *See* Dkt. 143 at Appx 1 (blue highlighting) and Dkt. 149 at 2. The chart also includes third parties with potential interest in the allegedly infringing projects and/or systems.

Final Compl. ¶¶	Projects Identified By Plaintiff	Remaining Patents & Claims	3d Parties with Potential Interest
156–157	Panasonic Toughbook + K-Max Helicopter (AACUS)	'891 Patent: claims 44, 45, 48, 52, 53, and 55	Boeing, which acquired AACUS Principle Investigator, Aurora Flight Sciences <sup>1</sup>  Lockheed Martin
171–172	iPad + Boeing MH-6 Little Bird (AACUS)	'891 Patent: claims 23, 27, 30, and 31	Boeing, which acquired Aurora Flight Sciences
214–215	Cell-All Synkera MikroKera Ultra	'497 Patent: claims 1, 2, 4	Integrated Device Technologies ("IDT"), which acquired Synkera Technologies Inc. in July 2016 <sup>2</sup>  Qualcomm
370–371	Eureka Aerospace High Powered Electromagnetic System (HPEMS)	'891 patent: claims 11, 15, 19, and 21	Eureka Aerospace

<sup>1</sup> See Press Release, <https://boeing.mediaroom.com/2017-11-08-Boeing-completes-acquisition-of-Aurora-Flight-Sciences>.

<sup>2</sup> See IDT Website, <https://www.idt.com/synkera-now-idt>.

Final Compl. ¶¶	Projects Identified By Plaintiff	Remaining Patents & Claims	3d Parties with Potential Interest
375–376	Laser Weapons System (LaWS)	'891 Patent: claims 11, 15, 19, 21	Kratos Defense & Security Solutions  Lockheed Martin  Northrop Grumman
380–381	ATHENA (Advanced Test High Energy Asset)	'891 Patent: claims 11, 15, 19, 21	Lockheed Martin
385–386	CHAMP (Counter-Electronics High- Powered Microwave Advanced Missile Project)	'891 Patent: claims 11, 15, 19, 21	Boeing  Raytheon
390–391	Northrop Grumman X-47B UCAS Control Display Unit (CDU)	'891 Patent: claims 11, 15, 19, 21	Northrop Grumman
395–396	Oshkosh Defense Autonomous Unmanned Ground Vehicle (UGV) “TerraMax”	'891 Patent: claims 44, 55	Oshkosh Defense
400–401	DreamHammer’s “Ballista” Software for Computer, Tablet or Smartphone	'891 Patent: claims 44, 55	DreamHammer Inc.
405–406	iControl Inc. “M-Lock”	'990 Patent: claims 125, 135	iControl (d/b/a Inteltyt <sup>3</sup> )

These projects vary widely in subject matter, including chemical sensing technology (*e.g.*, Synkera MikroKera Ultra), autonomous vehicle systems (*e.g.*, AACUS, X-47B UCAS, TerraMax, DreamHammer Ballista software), electronic conveyance locks (*e.g.*, mLOCK), and even energy weapons systems (*e.g.*, HPEMS, ATHENA, CHAMP, LaWS). Unsurprisingly,

<sup>3</sup> See Inteltyt Website, <http://intelyt.com/blog/2016/1/iconcontrol-incorporated-is-now-intelyt>.

these disparate projects/systems implicate a number of third parties that are either alleged to have been, or understood by the Government (based on its investigation to date) to have been, involved in the development, manufacture and/or sale of the accused systems.

Based on the numerous and varied allegations of the Final Complaint, the allegedly infringing projects or systems may have been designed, manufactured, and/or sold by the companies identified above. As a result, these companies may have an interest in appearing and defending its rights. *See, e.g., Allied Oil & Supply, Inc. v. United States*, 60 Fed. Cl. 223, 225–26 (2004) (noting that the interest requirement of Rule 14(b)(1) is broad, and that “an apparent interest is sufficient for notice to issue ‘[e]ven in those situations where an alleged third party interest in the suit is uncertain.’” (quoting *Del-Rio Drilling Programs, Inc. v. United States*, 17 Cl. Ct. 844, 849 (1989)). The issuance of the requested notice for each of the above-named entity conforms to the established practice of the United States Court of Federal Claims. *See, e.g., Carrier Corp. v. United States*, 534 F.2d 250, 251-52 (Ct. Cl. 1976); *Bowser, Inc. v. United States*, 420 F.2d 1057, 1060 (Ct. Cl. 1970); *Rockwell Int’l Corp. v. United States*, 31 Fed. Cl. 536, 539-40 (1994); *see also In re UUSI, LLC*, 549 Fed. Appx. 964 (Fed. Cir. 2013).

Recognizing that the Court previously suspended the Government’s deadline to file this notice (Dkt. 149 at 3), the Government files this motion with its Answer pursuant to RCFC 14(b)(2)(B)(ii) based on its investigation to date of Plaintiff’s remaining allegations of patent infringement.

## CONCLUSION


For the above reasons, the Government respectfully requests that this motion be granted and the requested notices be issued.

Respectfully submitted,

JOSEPH H. HUNT  
Assistant Attorney General

GARY L. HAUSKEN  
Director

March 18, 2019



---

NICHOLAS J. KIM  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
*Nicholas.J.Kim@usdoj.gov*  
T: (202) 616-8116  
F: (202) 307-0345

*Attorneys for the United States*




CERTIFICATE OF SERVICE

I hereby certify that a true copy of the foregoing "DEFENDANT UNITED STATES' MOTION FOR NOTICE" was deposited with Federal Express on March 18, 2019, postage pre-paid, to:

Larry Golden  
740 Woodruff Road  
#1102  
Greenville, SC 29607

Plaintiff, *pro se*

  
\_\_\_\_\_  
Nicholas J. Kim  
Department of Justice

# *Exhibit*

4

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN,

Plaintiff, *pro se*,

v.

THE UNITED STATES,

Defendant.

No. 13-307 C

Senior Judge Eric G. Bruggink

**DEFENDANT UNITED STATES' REPLY IN SUPPORT OF ITS  
MOTION FOR NOTICE**

The Government's Motion for Notice (Dkt. 162) should be granted, because it was timely filed under RCFC 14(b)(2)(B)(ii), and Plaintiff's response fails to identify any issues that should prevent interested parties from having the opportunity of being notified of Plaintiff's allegations in this case and deciding whether they will appear and defend any interests that they may have.

In opposition, Plaintiff contends that the Government's Motion for Notice is "untimely" for several reasons, none of which relate to RCFC 14:

1. "Plaintiff has not received all of the requested discovery documentation from the Government."
2. "Plaintiff has not received the requested list of alleged infringing products that 'does' and 'does not' have jurisdiction from the Claims Court."
3. "Plaintiff does not agree with the Government having the option to pick and choose which alleged infringing device to litigate."
4. "Count 1 'Takings' claims before Count 2 'Infringement' claims. Who authorized the Government to pick the direction of this case?"

Received - USCFC

APR 03 2019

Dkt. 164 (Plaintiff's Response to the Government's Motion for Notice in Case Number 13-107C, "Response") at 1. Plaintiff does not provide any support for these timing arguments. Instead, the majority of Plaintiff's paper is devoted to voicing continued displeasure over the Court's March 29, 2018 Order (Dkt. 130) dismissing a majority of Plaintiff's patent infringement claims, none of which is relevant to whether the Government's Motion for Notice should be granted. Resp. at 1–7. Plaintiff also suggests that notice has already been provided to several parties, including Qualcomm. *Id.* at 7. Finally, Plaintiff appears to condition grant of the Motion for Notice on non-parties answering Plaintiff's "FOIA request." *Id.* at 7. Taken separately or together, none of these reasons supports denial of the Government's Motion for Notice.

Beginning with the timing issue, Plaintiff's allegation that the Government's Motion for Notice is untimely is entirely unsupported under RCFC 14(b)(2)(B)(ii), the operative timing requirement of the Rule. The Government's Motion for Notice was filed on March 18, 2019, the same day that the Government filed its Answer (Dkt. 162) to the remaining allegations in Plaintiff's Final Complaint (Dkt. 120). *See* RCFC 14(b)(2)(B)(ii) ("The United States must file for notice on or before the date the answer is required to be filed."); *see also* Dkts. 130, 151 (dismissing certain allegations of Plaintiff's Final Complaint). Thus, the Government's Motion for Notice was timely.

As to the substantive requirements of RCFC 14, "[t]he key factor in every determination regarding the propriety of issuing notice is—whether the third party to whom notice is directed 'appears' to have an interest in the subject matter of the proceedings." *Del-Rio Drilling Programs v. United States*, 17 Cl. Ct. 844, 849 (1989). And "[e]ven in those situations where an alleged third party interest in the suit is uncertain, an *apparent* interest is legally sufficient to support an issuance of notice." *Id.* The parties named in the Government's Motion for Notice

correspond to the third party developers/suppliers named in the remaining allegations of Plaintiff's complaint. Therefore, the Government's Motion for Notice should be granted because it satisfies the requirements of RCFC 14.

Plaintiff's four enumerated "untimeliness" arguments are unpersuasive at least because they are entirely untethered to the requirements of RCFC 14. These are addressed in turn below.

*First*, RCFC 14 does not condition grant of the Government's motion on the start of "discovery."<sup>1</sup> In fact, by requiring such a motion be filed with the Complaint (by Plaintiff) or with the Answer (by Defendant), RCFC 14 clearly contemplates that the party would move prior to the start of discovery. *See* RCFC 14(b)(2)(B). *Second*, Plaintiff cannot prevent issuance of notice based on unreasonable, repeated demands that the Government provide a "list of alleged infringing products [over which the Court] 'does' and 'does not' have jurisdiction." This Court directed both parties to submit status reports identifying what, if any, patent infringement claims remained in this case. In response, Plaintiff repeatedly insisted that all of his patent infringement claims were dismissed. Yet at the same time, Plaintiff declined to move under RCFC 41 to dismiss any remaining claims to permit a prompt appeal of the Court's March 29, 2018 Order. Moreover, this Court's November 28, 2018 Order has set a path forward on the remaining claims, thereby mooting any vestige of Plaintiff's demand. *Third*, aside from being irrelevant to whether the Motion for Notice should be granted, Plaintiff cannot be heard to complain that the Government gets "the option to pick and choose which alleged infringing device to litigate," which is inaccurate and overlooks the fact that Plaintiff abdicated his right to influence the course of this litigation by repeatedly insisting that all of his patent infringement allegations had

---

<sup>1</sup> Discovery has not opened in this case. Prior to the Government's Partial Motion to Dismiss the Final Complaint (Dkt. 123), this Court permitted limited jurisdictional discovery, which has now concluded.

already been dismissed. *Fourth*, Plaintiff's unclear reference to his takings claims, which mirror the allegations in Plaintiff's patent infringement claims, actually supports granting the Motion for Notice.

Turning to Plaintiff's allegation that he "has already given notice to Qualcomm, Apple, Samsung, and LG because the [sic] Judge Braden has dismissed my patent(s) for lack of jurisdiction," Plaintiff has never filed any RCFC 14 notice in this case (*see* Dkt. 120, which was not accompanied by motion for notice under RCFC 14(b)(2)). Also, it is entirely unclear how the Court's March 29, 2018 Order would have provided such notice to Qualcomm or the other parties.<sup>2</sup> Similarly, Plaintiff's mere intent to file a complaint in the International Trade Commission cannot plausibly constitute notice under RCFC 14 of parties' potential interest in this case.

Lastly, Plaintiff cannot condition the grant of the Motion for Notice on companies answering his unidentified "FOIA request." To start, Freedom of Information Act ("FOIA") requests cannot be used to seek information from private entities like Raytheon, Boeing, Synkera, etc. And even when directed to the Government, the use of FOIA in litigation against the government is disfavored by the Court. *See Baldridge v. Shapiro*, 455 U.S. 345, 360 n.14 (1982) ("The primary purpose of the FOIA was not to benefit private litigants or to serve as a substitute for civil discovery."); *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978)

---

<sup>2</sup> The Government's Motion for Notice did not seek notice to be sent to Apple, Samsung or LG at this time, because the patent infringement allegations involving these three entities were understood to have been dismissed. *See* Dkts. 130, 151. Moreover, based on the Government's investigation to date, the Department of Homeland Security ("DHS") never entered into Cooperative Research and Development Agreements (CRADAs) with Qualcomm, Apple, Samsung and LG regarding the CELL-ALL project, which alleged agreements form the basis for Plaintiff's cell-phone-related infringement allegations. *See, e.g.*, Dkt. 162 (Gov't Answer) ¶¶50–51 (denying that the Government entered into the alleged CRADAs).

(“FOIA was *not* intended to function as a private discovery tool.”) (emphasis in original). Moreover, nothing in RCFC 14 contemplates conditioning notice on the receipt of information by the non-requesting litigant. In fact, the operation of RCFC 14 makes it more likely that Plaintiff will eventually receive information from third parties relevant to this case. Therefore, the Motion for Notice should be granted without Plaintiff’s requested condition.

### CONCLUSION

For the above reasons, the Government respectfully requests that its motion for notice be granted and the requested notices be issued.

Respectfully submitted,

JOSEPH H. HUNT  
Assistant Attorney General

GARY L. HAUSKEN  
Director

April 3, 2019



NICHOLAS J. KIM  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
*Nicholas.J.Kim@usdoj.gov*  
T: (202) 616-8116  
F: (202) 307-0345


*Attorneys for the United States*

**CERTIFICATE OF SERVICE**

I hereby certify that a true copy of the foregoing "DEFENDANT UNITED STATES'  
REPLY IN SUPPORT OF ITS MOTION FOR NOTICE" was deposited with Federal Express  
on April 3, 2019, postage pre-paid, to:

Larry Golden  
740 Woodruff Road  
#1102  
Greenville, SC 29607

Plaintiff, *pro se*

  
\_\_\_\_\_  
Nicholas J. Kim  
Department of Justice



# *Exhibit*

5

# In the United States Court of Federal Claims

LARRY GOLDEN,

No. 13-307 C

v.

UNITED STATES

COPY

## NOTICE

To: Qualcomm Inc.  
c/o The Prentice Hall  
Corporation System, Inc.  
251 Little Falls Drive  
Wilmington, DE 19808  
(302) 636-5400

Pursuant to Rule 14 of the Rules of the United States Court of Federal Claims, you are hereby notified of the above-captioned case in which you may have an interest in the subject matter. If you have an interest in the subject matter of this case, within forty-two (42) days after service of this Notice upon you, you may file a complaint or answer herein in accordance with Rule 14. For your information, this Notice is accompanied by copies of the following pleadings that have been filed herein: **Plaintiff's Complaint, Amended Complaint, and Defendant's Motion to Provide Notice to Interested Parties.**

In testimony whereof, I have hereunto set my hand and affixed the Seal of said Court at Washington, DC, this 22nd day of April, 2019.

Lisa L. Reyes  
U.S. Court of Federal Claims

By: Elin M. Hey  
Deputy Clerk

## RETURN OF SERVICE

Service of the above Notice was accomplished by forwarding same to the above named at the address indicated by registered or certified mail, return receipt requested. See return receipt attached showing service on \_\_\_\_\_.  
(Date)

\_\_\_\_\_  
Attorney of Record

# *Exhibit*

6

IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN,

Plaintiff, *pro se*,

v.

THE UNITED STATES,

Defendant.

No. 13-307 C

Senior Judge Eric G. Bruggink

**CERTIFICATE OF SERVICE ON QUALCOMM**

Pursuant to Rule 14(b) and the Court's April 16, 2019 order (Dkt. 166), the United States ("the Government") files with the Clerk its return of service on Qualcomm Inc., indicating completion of the required service of the Clerk's RCFC 14 Notice (*see* Dkt. 169). With the Notice, the Government also served Plaintiffs' Original Complaint (Dkt. 1), Plaintiff's Final Amended Complaint (Dkt. 120), and Defendant's Motion to Provide Notice to Interested Parties (Dkt. 161). A copy of the return receipt evidencing service of the original copy of the Notice is also filed with this certificate. *See* Exhibit 1.

Received - USCFC

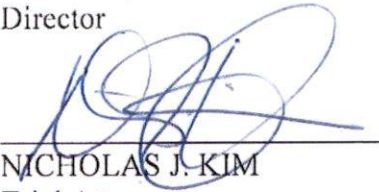
MAY 30 2019

Respectfully submitted,

JOSEPH H. HUNT  
Assistant Attorney General

GARY L. HAUSKEN  
Director

May 30, 2019



---

NICHOLAS J. KIM  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
*Nicholas.J.Kim@usdoj.gov*  
T: (202) 616-8116  
F: (202) 307-0345

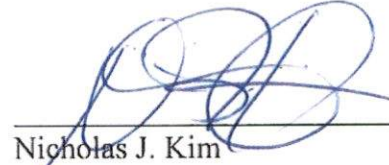
*Attorneys for the United States*

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the foregoing "CERTIFICATE OF SERVICE ON QUALCOMM" was deposited with Federal Express on May 30, 2019, postage pre-paid, to:

Larry Golden  
740 Woodruff Road  
#1102  
Greenville, SC 29607

Plaintiff, *pro se*



---

Nicholas J. Kim  
Department of Justice

# Exhibit 1

# In the United States Court of Federal Claims

LARRY GOLDEN,

No. 13-307 C

v.

UNITED STATES

## NOTICE

To: Qualcomm Inc.  
c/o The Prentice Hall  
Corporation System, Inc.  
251 Little Falls Drive  
Wilmington, DE 19808  
(302) 636-5400

Pursuant to Rule 14 of the Rules of the United States Court of Federal Claims, you are hereby notified of the above-captioned case in which you may have an interest in the subject matter. If you have an interest in the subject matter of this case, within forty-two (42) days after service of this Notice upon you, you may file a complaint or answer herein in accordance with Rule 14. For your information, this Notice is accompanied by copies of the following pleadings that have been filed herein: **Plaintiff's Complaint, Amended Complaint, and Defendant's Motion to Provide Notice to Interested Parties.**

In testimony whereof, I have hereunto set my hand and affixed the Seal of said Court at Washington, DC, this 22nd day of April, 2019.

Lisa L. Reyes  
U.S. Court of Federal Claims

By: Elin M. King  
Deputy Clerk

## RETURN OF SERVICE

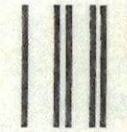
Service of the above Notice was accomplished by forwarding same to the above named at the address indicated by registered or certified mail, return receipt requested. See return receipt attached showing service on May 13, 2019.

(Date)

[Signature]  
Attorney of Record



UNITED STATES POSTAL SERVICE



First-Class Mail  
Postage & Fees Paid  
USPS  
Permit No. G-10

• Sender: Please print your name, address, and ZIP+4 in this box •

Nicholas J. Kim  
1100 L St. NW  
Washington DC 20005  
Room 8508



## SENDER: COMPLETE THIS SECTION

- Complete items 1, 2, and 3. Also complete item 4 if Restricted Delivery is desired.
- Print your name and address on the reverse so that we can return the card to you.
- Attach this card to the back of the mailpiece, or on the front if space permits.

1. Article Addressed to:

Qualcomm Inc.  
c/o The Prentice-Hall Corporation System,  
Inc.  
251 Little Falls Drive  
Wilmington, DE 19808

2. Article Number  
(Transfer from)

abel)

7014 2870 0000 7276 9833

## COMPLETE THIS SECTION ON DELIVERY

A. Signature

Paul Sisofo

☐ Agent  
☐ Addressee

B. Received by (Printed Name)

C. Date of Delivery

D. Is delivery address different from item 1? ☐ Yes  
If YES, enter delivery address below: ☐ No

3. Service Type

☐ Certified Mail ☐ Express Mail  
☐ Registered ☐ Return Receipt for Merchandise  
☐ Insured Mail ☐ C.O.D.

4. Restricted Delivery? (Extra Fee)

☐ Yes

PS Form

January 2004

Domestic Return Receipt

102595-02-M-1540

# *Exhibit*

*7*

# In the United States Court of Federal Claims

No. 13-307C  
(Filed: March 29, 2021)

\*\*\*\*\*

LARRY GOLDEN,

*Plaintiff,*

v.

THE UNITED STATES,

*Defendant.*

\*\*\*\*\*

## ORDER

Before the court is defendant's March 12, 2021 motion (ECF No. 216) to issue notice to Apple Inc. ("Apple"), LG Electronics, Inc. and LG Electronics U.S.A., Inc. (collectively, "LG"), and Samsung Electronics Co. and Samsung Electronics America, Inc. (collectively, "Samsung") that these entities may file appropriate pleadings if so desired and assert whatever interest each may have in this action. Also pending is plaintiff's March 15, 2021 motion (ECF No. 218) for a more definite statement filed in response to defendant's motion, and defendant's March 26, 2021 reply (ECF No. 219) to plaintiff's response.

The government argues that notice should be issued to Apple, Samsung, and LG because these entities may have an interest to assert in this case pursuant to plaintiff's sixth amended complaint. ECF No. 195 (Sixth Am. Compl.). In support of its argument, defendant cites to plaintiff's sixth amended complaint, which suggests that government use of various consumer electronic devices developed, manufactured, and sold by Apple, Samsung, or LG infringes the patents asserted in plaintiff's sixth amended complaint.<sup>1</sup> Accordingly, defendant argues the need for notice to Apple,

---

<sup>1</sup> Defendant's motion to cites to ECF No. 195 at 132 (Sixth Am. Compl.); *see also, e.g.*, ECF No. 195 at 5 (referring to "261 million CMDC devices

Samsung, and LG to appear, if they so desire, as parties and assert whatever interest they may have.

In response, plaintiff requests a more definite statement, arguing that defendant's motion is "so vague and ambiguous" that plaintiff cannot respond (ECF No. 218 at 1) and further that plaintiff "has patent claims that covers a communicating, monitoring, detecting, and controlling (CMDC) device that he believes antedates the release date of the Cell-All initiative that solicits the consumer devices of Apple, Samsung, and LG used as an inventive process in the development and manufacture of the Cell-All devices." ECF No. 218 at 4.

In reply, defendant opposes plaintiff's motion on two grounds. First, defendant argues that plaintiff's response is procedurally improper pursuant to Rule 12(e) of the Rules of the United States Court of Federal Claims, which permits a motion for a more definite statement of a pleading, but not a motion. Second, defendant contends that plaintiff's allegations regarding Apple, Samsung, and LG are factually inaccurate.

We treat plaintiff's motion for a more definite statement as opposition to defendant's motion to notice interested third parties. As to defendant's claim that plaintiff's allegations are factually accurate, we need not reach a conclusion at this stage. We are satisfied that good cause has been shown to issue notice based on the allegations made in plaintiff's sixth amended complaint. Specifically, plaintiff alleges that his "communicating, monitoring, detecting, and controlling ("CMDC") device is commercialized in the form of an improved cell phone, smartphone, smartwatch, laptop, or tablet . . . the specifications and capabilities of the CMDC devices that were developed for, manufactured and commercialized by third-party government contractors, Apple, Samsung, and LG, are significantly the same as the Plaintiff's CMDC devices." Sixth Am. Compl. ¶¶ 6, 12. Attached to the sixth amended complaint is a claim chart that purports to identify features of devices alleged to be part of the DHS Cell-All initiative that infringe claims of the patents asserted in the current complaint. *Id.* Ex. 7 (claim charts for

---

(i.e. smartphones)" as infringing products), 85–93 (discussing alleged general government use of commercially available Apple, Samsung, and LG consumer smartphone and tablet devices under the heading "Government's 'use' of Plaintiff's CMDC device"). ECF No. 216 at 3 (Def.'s Third Mot. to Notify Interested Party).

the DHS Cell-All initiative). As such, Apple, Samsung, and LG may be noticed in order to assert whatever interest they may have.

Previously, we granted the government's first motion to issue notice to IDT because IDT was identified as having an interest in the Cell-All Project,<sup>2</sup> a project which allegedly infringes plaintiff's 7,385,497 patent. On March 30, 2019, IDT was acquired by Renesas and began operating under the name Renesas on January 1, 2020. ECF No. 198. We granted the government's second motion to issue notice to Renesas because on March 30, 2019, IDT was acquired by Renesas and began operating under the name Renesas on January 1, 2020. ECF No. 198. Based on the representations made in the government's third motion (ECF No. 216), the court grants the government's motion to issue notice and denies plaintiff's motion for a more definite statement (ECF No. 218). The Clerk of Court is directed, pursuant to Rule 14(b)(3) of the Rules of the United States Court of Federal Claims, to issue notice to Apple, Samsung, and LG to assert whatever interest the companies may have in this action.

s/Eric G. Bruggink  
ERIC G. BRUGGINK  
Senior Judge

---

<sup>2</sup> Plaintiff alleges the Department of Homeland Security's project named "Cell-All" (Cell-All Project) infringes plaintiff's '497 patent. ECF No. 195 at 7-8 (¶¶10-12).

# *Exhibit*

8



# IN THE UNITED STATES COURT OF FEDERAL CLAIMS

LARRY GOLDEN,

Plaintiff,

V.

UNITED STATES,

Defendant.

1:13-cv-307-EGB

Senior Judge Eric G. Bruggink

March 27, 2021

## **PLAINTIFF'S STATUS REPORT AND LEAVE OF THE COURT TO FILE A MOTION FOR DEFAULT JUDGEMENT**

Pursuant to this Court's order, filed 02/26/2021 in this Case No. 13-307C; Dkt. No. 215, Plaintiff ("Larry Golden") is filing this "Status Report".

The Court of Federal Claims follows the precedent of the Court of Claims and of the United States Court of Appeals for the Federal Circuit, of determining if there is infringement before allowing a challenge to the validity of a patent. *See South Corp. v. United States*, 690 F.2d 1368, 1369, 215 U.S.P.Q. (BNA) 657 (Fed. Cir. 1982). Compare *Gargoyles, Inc. v. United States*, 26 Cl. Ct. 1367, 1369 (1992) (stating "[T]his court need consider the [patent] validity arguments only if infringement is found" *See Barrett v. United States*, 405 F.2d 502, 510, 160 U.S.P.Q.2 (BNA) 224 (Ct. Cl. 1968) ("Since there is no infringement, it is unnecessary to decide validity."); *Autogiro Co. v. United States*, 384 F.2d 391, 415 (Ct. Cl. 1967) ("Only on claims found infringed is it necessary to reach a decision on validity.")).

Following the Court of Claims' rationale, however, the Federal Circuit developed the practice of vacating validity findings upon an affirmance of noninfringement, citing the rationale that a court need not consider validity if no infringement exists. *See, e.g., Vieau v. Japax, Inc.*, 823 F.2d 1510, 1517, 3 U.S.P.Q.2d (BNA) 1094 (Fed. Cir. 1987) (dismissing cross-appeal on invalidity as moot); *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1571, 1

Received - USCFC

MAR 29 2021

U.S.P.Q.2d (BNA) 1881 (Fed. Cir. 1986) (criticizing custom of proving validity prior to deciding infringement). *See Unette Corp. v. Unit Pack Co.*, 226 U.S.P.Q. (BNA) 715, 717 (D.N.J. Mar. 8, 1985) (rendering validity issue moot upon finding of noninfringement)

District courts, as well as the Court of Federal Claims, have adopted this practice on the trial level as well. *See Gargoyles*, 26 Cl. Ct. at 1369 (rendering validity issue extraneous upon finding of noninfringement); *Unette Corp. v. Unit Pack Co.*, 226 U.S.P.Q. 715, 717 (D.N.J. 1985) (rendering validity issue moot upon finding of noninfringement), *affd*, 785 F.2d 1026, 228 U.S.P.Q. (BNA) 933 (Fed. Cir. 1986). In contrast to making the validity of a patent moot following a finding of noninfringement, the sole issue at the trial level is whether a court should review validity at the trial level upon a finding of noninfringement. *See Howard T. Markey*, On Simplifying Patent Trials, 116 F.R.D. 369, 370-71, 380-81 (1987) (considering role of trial courts as fora for validity determinations in absence of infringement).

For the reasons stated above and in accordance with the well-established precedent of this Court of Federal Claims and the Federal Circuit Court, Plaintiff is asking this Court to adopt and follow the schedule below for future proceedings. Plaintiff finds the Government proposed schedule as being very deceptive. First, Plaintiff has satisfied the “preliminary disclosure of infringement contentions; second, there is no call for an infringement analysis; and third, the Government is asking for five months to cover claim construction, when the Court has not decided if there’s anything left to construe.

In the first step of the infringement analysis... a court determines what is patented. In the second step of the analysis... the court ascertains whether the accused device embodies every element of the claim. Even if the accused device fails to embody every literal detail of a claimed invention, however, it may infringe the patent if it constitutes a substantially equivalent embodiment of the patented invention. *Deuterium Corp.*, 16 Cl. Ct. at 461. The classic “doctrine of equivalents” asks whether the accused process “performs substantially the same function in substantially the same way to obtain the same result” as the patent claim. *Graver Tank & Mfg. Co. v. Linde Air Prods. Co.*, 339 U.S. 605, 608, 85 U.S.P.Q. (BNA) 328 (1950) (quoting *Sanitary Refrigerator Co. v. Winters*, 280 U.S. 30, 42 (1929)).

The basis for Plaintiff to file this status report at this time is to first, conform with history in which the Court of Federal Claims follows the precedent; second, to reduce the amount of time and cost of repeating the same challenges to the same subject matter specifications that was



covered in ordinary patent examinations; re-issue patent examinations; and *inter partes* review (IPR). Below is Plaintiff's proposed schedule:

Event	Date
Government's Response to Plaintiff's Preliminary Disclosure of Infringement Contentions—Claim Charts (Exhibit 7 of Amended Complaint)	April 19, 2021 (21 days after filing Status Report)
Plaintiff's Reply to the Government's Response to Plaintiff's Preliminary Disclosure of Infringement Contentions as a Final Disclosure of Infringement Contentions	May 10, 2021 (20 days after Government files its Response)
Government's Response to Plaintiff's Final Disclosure of Infringement Contentions	May 31, 2021 (21 days after Final Disclosure of Infringement Contentions)
Plaintiff's Reply to the Government's Response to Plaintiff's Final Disclosure of Infringement Contentions	June 21, 2021 (21 days after Government files its Response)
Court issues an Opinion on Infringement and/or Non-Infringement	Court's discretion
TITLE V. SETTLEMENT; Rule 16 – Mandatory Settlement Discussions	Within 7 days after the Court's Opinion

According to the Order filed 02/26/2021 in Case No. 13-307C; Dkt. No. 215, "In alleging infringement of his patented CMDC technology, plaintiff attached a lengthy series of "claim charts" illustrating allegations of how the government, and third parties at the government's behest, are infringing certain of his patents' claims. Sixth Am. Compl. Ex. 7 at 100-108. Defendant's motion has not attempted to wrestle with that chart or otherwise explain with any detail why those claims fail as a matter of law." Plaintiff has included as **Exhibit A**, a copy of Exhibit 7 of the Sixth Amended Complaint.

The Government explains its position in an e-mail correspondence with the Plaintiff, stating:

"Further, given your statements below, it does not appear that further e-mail correspondence on these issues will be productive at this point. Having said that, I would like to correct some of the statements in your e-mail below for the record. To be clear, there were no "new and improved cell phones" developed or manufactured as part of the

Department of Homeland Security's "CELL-ALL" project. Nor did the Government "impliedly enter into a contract" with any of Apple, Samsung, or LG as part of the CELL-ALL project. As explained in our Answers filed in this case, the CELL-ALL project culminated in a September 28, 2011 demonstration in Los Angeles, at which two separate prototype units were exhibited—one developed by NASA, and another developed by Qualcomm. Those two prototype units were the only devices developed as part of the CELL-ALL project, which concluded nearly a decade ago. The Government has moved for notice to be issued to Apple, Samsung, and LG not because they were contractors on the CELL-ALL project (they were not), but because you have alleged that *any* Government use of these companies' consumer electronics devices infringes your asserted patents (**Exhibit B**)

Included in the e-mail correspondence is the Government's proposed schedule. A copy of the schedule is illustrated below.

Event	Date
Government's Answer	March 12, 2021
Plaintiff's Preliminary Disclosure of Infringement Contentions (Patent Rule 4)	May 7, 2021 (56 days after filing of Answer)
Government's Preliminary Disclosure of Invalidity Contentions (Patent Rule 6)	July 2, 2021 (56 days after Preliminary Infringement Contentions)
Parties exchange list of claim terms proposed for construction (Patent Rule 9)	August 13, 2021 (42 days after Preliminary Invalidity Contentions)
Parties exchange proposed constructions (Patent Rule 10)	September 10, 2021 (28 days after exchange of list of proposed claim terms)
Parties file joint claim construction chart, appendix, and prehearing statement (Patent Rule 11)	October 15, 2021 (35 days after exchange of proposed constructions)
Parties file respective opening claim construction briefs (Patent Rule 15(b)(1))	December 10, 2021 (56 days after filing of joint claim construction chart)
Parties file respective responsive claim construction briefs (Patent Rule 15(b)(2))	January 7, 2022 (28 days after filing of opening claim construction briefs)
Claim Construction Hearing, if requested by the Court	At the Court's convenience

Plaintiff believes the Defendant's deceptive schedule is designed to do nothing more than continue wasting this Court's time. Example: "56 days for Plaintiff to submit Plaintiff's preliminary infringement contentions." The Government should have responded to Plaintiff's preliminary infringement contentions in its Motion to Dismiss. Even after this Court cautioned

the Government in the Court's order, "Defendant's motion has not attempted to wrestle with that chart", the Government elected not to respond to the chart when the Government submitted its answer (Dkt. 217) to Plaintiff's complaint. But yet, the Government wants the Plaintiff to spend another 56 days doing something Plaintiff has already done, and according to the Government's proposed schedule, the Government doesn't plan to respond after Plaintiff submits another, or the same, "preliminary infringement contentions".

Plaintiff is seeking leave of this Court to file a "Motion for Default Judgement". **Default Judgment** – Failure to take action can result in this binding judgment by a court in favor of the other party. *Example:* If the defense fails to respond to a complaint and does not provide an answer in a certain timeframe, the plaintiff may take an additional step: filing a motion for default judgment. Once the motion is filed, the court may then choose to issue a default judgment in favor of the plaintiff, since the defense failed to take the required actions."

## **GOVERNMENT DESIGNED "CONSUMER DEVICES" FOR 260 MILLION CONSUMERS**

Three main changes to the 2007 cell phone or smartphone that makes it a new and improved cell phone or smartphone, made available for CBRN&E detection are: the central processing unit (cpu) that is considered by many as the "brain" of the devices; the operating systems that are considered by many as the "mind" of the devices; and, the wireless protocols (i.e., Bluetooth, cellular, Wi-Fi, radio-frequency (RF))

"In order for the Cell-All public safety sensing and alerting system to be complete, four links must be forged and joined together: the sensor and computing hardware, the sensing application for mobile phones, a centralized server and network operations center, and the end consumer, whether individuals, emergency operations centers, first responders, government agencies, or private companies. Both Synkera and NASA are independently producing sensors—with Synkera developing a stand-alone sensing card and NASA creating a nanosensor-embedded "sleeve" for phones—that will detect chemicals in the immediate environment and communicate those readings via Bluetooth, or other protocols, to phones (Li, 2011; Synkera Technologies, 2011)."

Therefore, connecting a Synkera stand-alone sensing card is accomplished the same as connecting a smartwatch to a smartphone. Which means the smartphones are ready for connecting 260 million smartphone users to a detection device. “To use a smartwatch (i.e., stand-alone detection device), you need a smartphone. On your smartphone, you install the app that comes with the smartwatch (i.e., stand-alone detection device), such as Android Wear (Wear OS—operating system from Samsung’s Tizen software) or Watch from Apple (i.e., watchOS 7—operating system). By opening the accompanying app on your smartphone and turning on Bluetooth, you can synchronize the watch (i.e., stand-alone detection device) with your phone.”

**Smartphones Could Form Chemical Detection Networks (By Jeremy Hsu, Nov. 2009)**



The chemical sensing prototype **plugged into an iPhone 30-pin dock connector** with the display-side up. (Image credit: Dominic Hart/NASA) Smartphones... **double as chemical sensors that can transmit alerts** to first responders about the release of dangerous chemicals. A NASA scientist has unveiled a postage-stamp-sized sensor that can **plug into an iPhone** and convert Apple's... **product into a mobile chemical detector**. The tiny device can sniff out low amounts of ammonia, chlorine gas and methane, and **send alerts to other phones or computers over regular phone networks or a Wi-Fi connection**. "Ours is the smallest in the world that can do complete sensing work," said Jing Li, a physical scientist at NASA's Ames Research

Center in California. Li and other researchers developed the proof of concept for the Department of Homeland Security's Cell-All program. Homeland Security hopes to eventually see such **sensing chips embedded in everybody's cell phone**, so that the **mobile devices could form a huge chemical-alert network** wherever people go. Having continuous use with the sampling jet cuts the battery endurance down to around 20 hours; convert the sensing chip's electronic signal from voltage to frequency, so that **the iPhone's wave recorder could register the sensor data**. They even plan on the **data including pinpoint locations of the chemical events, courtesy of GPS on the iPhone**. *(Everything in bold above means an adaptation or modification was made to the 2007 cell phone or smartphone to make it a new and improved cell phone or smartphone that is available to 260 million users for CBRN&E detection).*

The Government requested the development and manufacture for the Government, 260 million new and improved cell phones or smartphones (i.e., my CMDC devices), **“capable of”** CBRN&E detection. It doesn't matter that the Cell-All project only produced two prototypes. What matters now is the 260 million new and improved cell phones or smartphones that are **“capable of”** and currently ready to be used as chemical detectors, as a result of the Cell-All initiative that reads on the 28 claims of my CMDC device asserted in this case.

### **IMPROVEMENT PATENTS**

Most of the patent claims Plaintiff has asserted in this case falls into the category of a “new and improved” invention over that of a regular utility invention. Most of the improvement patent claims are stated as:

“A communication device of at least one of a cell phone, a smartphone, a desktop, a handheld, a personal digital assistant (PDA), a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:” or, “Monitoring equipment of at least one of the products grouped together by common features in a product groupings category of design similarity comprising of a computer terminal, personal computer (PC), laptop, desktop, notebook PC, handheld, cell phone, personal digital assistant (PDA) or smart phone interconnected to a product for communication therebetween, the monitoring equipment comprising:”

An improvement patent is one that's sought by an inventor who has not invented something that is completely original but rather builds upon an existing invention. Most patents are classified as improvement patents. When patenting an improvement to an existing invention, the patent office looks at whether the improvement to an existing invention is meaningful, new, non-obvious, and useful. If an inventor is able to patent his improvement, he will be able to stop everyone, including the inventor of the original invention from making, selling, and importing the invention as improved to the United States.

An individual would apply for an improvement patent the same way they would apply for any patent. An improvement patent is applied for using a regular utility patent application. To obtain an improvement patent, the invention must satisfy the patenting requirements set forth by the USPTO. During the 20-year patent term, the patent holder will be able to stop others from using, making, selling, and importing the patented invention to the United States without first obtaining the patent holder's expressed permission.

As equally important, Plaintiff has asserted regular utility patent claims in this case. A regular utility patent is one that sought for an original invention that has never been patented nor has been publicly disclosed. Plaintiff's communicating, monitoring, detecting, and controlling (CMDC) device has never been patented nor has been publicly disclosed, and is stated in Plaintiff's patent claims as:

"A communication device comprising: at least one central processing unit (CPU); at least one motion sensor in communication with the at least one CPU; at least one viewing screen for monitoring in communication with the at least one CPU; at least one global positioning system (GPS) connection in communication with the at least one CPU; at least one of an internet connection Wi-Fi connection in communication with the at least one CPU; at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU; at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device; at least one power source comprising of at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device; at least one biometric sensor in communication with the at least

one CPU for providing biometric authentication to access the communication device; at least one or more detectors in communication with the at least one CPU for detecting at least one of a chemical, biological, radiological, or explosive agents; at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU; and at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of, a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of, a building, or send signals to detect at least one of a chemical biological, radiological, or explosive agent such that *the communication device is capable of communicating, monitoring, detecting, and controlling.*”

Plaintiff’s “new and improved” cell phone, smartphone, desktop, handheld, personal digital assistant (PDA), laptop, or computer terminal, are not recognized in the above quoted patent claim because the communication device (CMDC device) stands on its own as an original utility invention.

Therefore, the argument is not whether Plaintiff has a “new and improved” cell phone, smartphone, etc. The argument is whether the products manufactured for or used by the Government infringes each and every patent claim limitation of at least one of Plaintiff’s independent patent claims asserted in this case. But, because the Defense can’t see this, makes it impossible to work with the Defendant on a status report going forward. Plaintiff recommends going forward with determining if there is infringement or non-infringement. If there’s no infringement, a challenge to Plaintiff’s patent(s) validity and claim construction is not necessary.

## **THE GOVERNMENT IMPLIEDLY ENTERED INTO CONTRACTS WITH APPLE, SAMSUNG, AND LG**

*Judge Braden. Memorandum Opinion and Order Denying the Government's Motion to Dismiss: Larry Golden v. The United States; Case 1:13-cv-00307-SGB Document 94 Filed 11/30/16.*

“Moreover, “authorization or consent of the Government,” does not need to be expressly stated. *See TVI Energy Corp. v. Blane*, 806 F.2d 1057, 1060(Fed. Cir. 1986)

("[a]uthorization or consent by the Government can be express [or] [i]n proper circumstances, Government authorization can be implied."). Indeed, "authorization or consent . . . may be given in many ways other than by . . . direct form of communication—e.g., by contracting officer instructions, [or] by specifications . . . which impliedly sanction and necessitate infringement["] *Hughes Aircraft co*, 534 F.2d at 901."

"Based on the alleged facts, the court can reasonably infer that iControl is a government contractor and that the manufacture and use of M-Lock was "for the benefit of [DHS]." *see Advanced Software Design Corp.*, 583 F.3d at 1378. In light of the allegation that the inventions disclosed in patents '752 and '990 were designed to prevent terrorist activity, it is plausible that iControl manufactured an infringing device for the benefit of DHS to promote national security, *see, e.g., Hughes Aircraft Co.*, 534 F.2d at 898 (finding that the government's participation in a satellite program was "for the Government," because the program was vital to the military defense and security of the United States). Moreover, under section 1498(a), "Government authorization or consent" can be implied by circumstances. *See TVI Energy Corp*, 806 F.2d at 1060."

"In light of these allegations, the court can reasonably infer that Eureka Aerospace's manufacture and use of the HPEMS advances the military defense and security of the United States and is thus... "for the benefit of the Government." *see, e.g., Hughes Aircraft co.*, 534 F.2d at 898. Moreover, construed in the light most favorable to Plaintiff, the February 12, 2016 Amended Complaint alleges that USAF contracted with Eureka Aerospace to develop and commercialize the HPEMS—sufficient facts to support a reasonable inference that USAF implicitly authorized the manufacture and use of the infringing device. *See TVI Energy Corp.*, 806 F.2d at 1060."

"The February 12, 2016 Amended Complaint's NSF claims also allege sufficient facts to plausibly establish that the use of the accused devices was "with the authorization or consent of the Government." Authorization or consent can be implied from the circumstances—"e.g., by contracting officer instructions, [or] specifications or drawings which impliedly sanction and necessitate infringement." *Hughes Aircraft Co.*, 534 F.2d at 901. For example, in *TVI Energy Corp.*, the United States Court of Appeals for the Federal Circuit held that the Government impliedly sanctioned the use of a patented invention when it issued a solicitation that required bidders to submit for inspection, and



perform live demonstrations of, the accused device. *See TVI Energy Corp.*, 806 F.2d at 1060.”

“In this case, the relevant NSF grants anticipate that the awardees will develop and test the devices proposed in their applications. *See, e.g.*, NSF Award No. 1444240 (“Annual and Final project reports, as required in the NSF Grant Conditions, should document all efforts and outcomes, whether or not they are successful.”). Government funding of research that will lead to the development and testing of an accused device supports a reasonable inference that the Government impliedly sanctioned infringing activity.”

## **MOBILE DEVICE SECURITY FOR “GOVERNMENT USERS”**

### **Message:**

“I am pleased to submit the following report, ‘Study on Mobile Device Security,’ which was prepared by the Department of Homeland Security (DHS) in consultation with the National Institute of Standards and Technology (NIST). This report was prepared pursuant to Section 401 of the Cybersecurity Act of 2015 (Consolidated Appropriations Act of 2016, Div. N, § 401, Pub. L. 114-113, 129 Stat. 2244, 2977-78 [2015]). Pursuant to congressional requirements, this report is being provided to the following Members of Congress: The Honorable Orrin Hatch, President Pro Tempore of the Senate; and, The Honorable Paul Ryan, Speaker of the House.” Department of Homeland Security / “*Study on Mobile Device Security*” / Message from the Under Secretary (Acting) for Science and Technology, April 2017. (Exhibit C)

### **Executive Summary:**

“Threats to the Government’s use of mobile devices are real and exist across all elements of the mobile ecosystem... the typical use of the devices outside the agency’s traditional network boundaries requires a security approach that differs substantially from the protections developed for desktop workstations... For the purposes of this study, the term “mobile device” refers to smartphones and tablets running mobile operating systems, as defined in NIST Special Publication 800-53, Revision 4. Mobile phones and the subclass of smartphones represent one of the greatest advances in human

communication in history... According to the Global System for Mobile Alliance (GSMA), the professional body composed of most carriers, mobile network operators and equipment makers, penetration in 2015 reached 4.7 billion unique subscribers globally. By 2020 that number is expected to reach 5.6 billion, meaning that over 70 percent of the world's population will have a mobile subscription... The stakes for government users are high. Government mobile devices... represent an avenue to attack back-end systems containing data on millions of Americans in addition to sensitive information relevant to government functions... Threats range from advanced nation state attacks, to organized crime using advanced fraud technologies, to simple theft of mobile phones. The threats to government users of mobile devices include the same threats that target consumers, e.g., call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data... This report addresses each element of the ecosystem with sections providing a detailed summary of the greatest threats in each area as well as current mitigations and defenses. The threat model is examined in detail with further delineation in the newly published draft NIST Interagency Report 8144, *Assessing Threats to Mobile Devices & Infrastructure: The Mobile Threat Catalogue*... The Government should select mobile devices and enterprise mobility management products that have been evaluated to meet a minimum level of security, e.g., the NIAP Product Compliant List or other Government approved product lists. NIAP approved products must be considered in the context of the environment of use, including appropriate risk analysis and system accreditation requirements. Customers must ensure that the products selected will provide the necessary security functionality for their architecture... These solutions will require collaboration between the public and private sectors to address the needs of the Government for increased mobile security but the solutions will not solely benefit the Government... The Department of Homeland Security is responsible for safeguarding the American people, our homeland, and our values. The threats detailed in this paper to cybersecurity in general and mobile security in particular pose serious challenges to the security and resilience of the Nation.

**Security features for DHS's new and improved mobile devices:**

“Mobile devices generally use an isolated execution environment such as a Trusted Execution Environment (TEE) (on Android and some other devices) and Apple’s Secure Enclave (on Apple iOS devices) that runs independently from the main operating system (e.g., Android or iOS). These environments provide security-critical capabilities such as storing cryptographic keys, including the keys used to encrypt sensitive data stored on the mobile device. Moving security-critical capabilities to an isolated execution environment provides *resilience against attacks that successfully exploit the main operating system.*” “Security requires integrity from individual components and also how they work together as an integrated system. *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

“Table 2. Available Defenses to Mitigate Attacks Against Device Components: Acquire only devices that meet security criteria—Seek commitments from the device vendor or mobile carrier at procurement to provide security updates in a timely manner and continue security update support for a set period. *Use strong authentication mechanisms*—even when available—for cloud services on which the device depends for secure functionality. Only purchase devices with secure boot capabilities and other critical security features, e.g., as defined in NIAP’s Mobile Device Fundamentals Protection Profile.” *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

“Google has implemented a version of this strategy with *Smart Lock, which uses information about trusted Bluetooth devices, trusted places, and on-body detection* to reduce the number of required manual screen unlocks. Google had previously determined that many users avoid use of a passcode for screen lock due to the number of times the screen had to be unlocked throughout the day...” “The recent addition of fingerprint sensors to many mobile devices has encouraged users to set a screen lock passcode since having a passcode is required for enabling the fingerprint sensor. Adrian Ludwig of Google’s Android Security Team reported that the use of the lock screen has increased from around 50 percent to 90 percent on *Android devices with a fingerprint sensor.*

Apple's Touch ID has likely had similar effects on iOS devices. *Apple and Google have added activation lock capabilities to their mobile devices that prevent lost or stolen devices from being factory reset...* *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

"To combat USB attacks, iOS and Android devices now require the mobile device user to explicitly trust any new PC to which the device has not previously connected. The device screen must be unlocked to establish the trust... The most important action to defend against physical threats is to ensure that *mobile devices always have a screen lock PIN or password*. If there is not a screen lock, it is easy for an attacker to access the data or functionality of a lost or stolen mobile device. Enrolling devices into an EMM system provides an enterprise the ability to enforce use of a screen lock... On iOS devices, Apple's Device Enrollment Program can be used to automatically enroll enterprise-owned devices into enterprise management and ensure the devices cannot be removed from management." *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

"III.1 Approach to Mobile Security: As depicted in Figure 2, these unique attributes include their almost always powered-on state, ubiquitous network connectivity, multiple radio interfaces (cellular, Wi-Fi, NFC, Bluetooth), and inclusion of a wide variety of sensors including biometric, GPS, compass, gyroscope, barometer, camera, and microphone array. These properties mean a desktop approach to security is not sufficient..." "There is a need for additional efforts and education to encourage users to enable screen lock on their devices regardless if a PIN, gesture, or biometric is used to protect it. Existing strong authentication solutions are not designed to complement the mobile form factor. More research is needed that incorporates the unique sensor data (motion sensor/ accelerometer, gyroscope, GPS, force sensor, capacitive sensor and camera) *captured by the device to uniquely identify the registered device user.*" *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

“The ‘RAN’ is the part of the mobile network that connects mobile subscribers to their service provider network using Radio Frequency (RF) signaling over an “air interface,” i.e., wirelessly. The RAN typically includes tower antennas, RF transceivers and RF controllers. To protect the privacy of callers, this part of the service is typically encrypted, although the level of encryption varies from network type to network type and by decisions the carrier makes in implementing this capability. Different levels of protection exist and vary widely by country...” “Near Field Communication Forum (NFC Forum). NFC is a set of communication protocols developed by the NFC Forum. It is designed to enable data exchanges at extremely close ranges (less than 3 inches). The integration of NFC technology into mobile devices is increasing because it enables an expanding number of capabilities. NFC is designed such that security can be integrated at multiple points in the protocol stack.” *DHS Study on Mobile Device Security - April 2017 - FINAL*

<https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

**Security features for Apple, Samsung, LG, and Qualcomm’s new and improved mobile devices:**

As described in Section IV.2.1, mobile device vendors have taken novel approaches to security architectures beyond the traditional approaches of desktop personal computers (PCs). Additionally, the National Information Assurance Partnership (NIAP) has had great success collaborating with the mobile industry through its Mobility Technical Community to develop technology-specific security requirements for mobile devices and mobile device management solutions. Numerous vendors, including Apple, Boeing, LG, Microsoft, MobileIron, and Samsung have successfully taken mobility products through Common Criteria evaluations against these requirements. For more information concerning NIAP and the security requirements documentation, refer to Section III.2. *DHS Study on Mobile Device Security - April 2017 - FINAL*

<https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

These security architecture improvements across all the mainstream mobile and PC operating systems (Google’s Android and Apple’s iOS as well as Microsoft’s

Windows and other operating systems) are to be encouraged and applauded because they increase resilience to attack and raise the level of difficulty and the cost for attackers to discover vulnerabilities and develop exploits. *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

Some individual Android vendors have incorporated their own security features in addition to what Google provides. For example, many of Samsung's Android devices feature additional security capabilities such as their Real-time Kernel Protection (RKP) feature and TrustZone-based Integrity Measurement Architecture (TIMA) to detect and respond to indications of device compromise... *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

Security requires integrity from individual components and also how they work together as an integrated system. Without a secure platform, you cannot have privacy—it would be possible to have a secure device that does not address privacy, but not the other way around. *Qualcomm / DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

Rogue base stations can also interfere with network-assisted location services by failing to interoperate with the service correctly. GPS units in smartphones need this service to quickly and reliably determine their location. This would mean both the mobile phone and the emergency call center would lack adequate location information to dispatch services. *DHS Study on Mobile Device Security - April 2017 - FINAL* <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf>

**GOVERNMENT INITIATIVES FOR A “NEW AND IMPROVED  
“CELL PHONE, SMARTPHONE, TABLET**

**(i.e., PLAINTIFF'S CMDC DEVICES)**

1. The U.S. Government Accountability Office: According to the most recent OMB estimate, the federal government spends about \$1.2 billion annually on about 1.5 million mobile devices and associated services. View GAO-15-431. For more information, contact Carol R. Cha at (202) 512-4456 or chac@gao.gov.

2. Beginning in year 2008 and continuing, the "Government" has given authorization and consent through contracts, agreements, grants, and procurements, to at least the mobile device manufacturers and developers of Apple, Samsung, Qualcomm, LG, Motorola, and Panasonic for the development and manufacture of mobile devices to be used by and for the "Government". All contracts, agreements, and procurements were made with the mobile device manufacturers Apple, Samsung, Qualcomm, LG, Motorola, and Panasonic after the Patent Owner gave notice to the "Government" between the years 2006 and 2007. See Plaintiff's discovery production at Section VII., A-E; and Docket No. 101 for the following:

3. 2008: "DHS S&T is pursuing what's known as cooperative research and development agreements with four cell phone manufacturers: Qualcomm, LG, Apple, and Samsung. These written agreements, which bring together a private company and a government agency for a specific project, often accelerate the commercialization of technology developed for government purposes." Quote taken directly from the Department of Homeland Security's website.

4. 2008: "During the demonstration, chemical readings captured from the simulated scenarios as well as location data are transmitted to the test network. The cell phone number is also transmitted; however, this information is scrubbed by the cell phone provider (per agreements with S&T) and is not displayed in the final output."

5. 2012: "The U.S. Department of Defense expects in coming weeks to grant two separate security approvals for Samsung's Galaxy smartphones, along with iPhones and iPads running Apple's latest operating system—moves that would boost the number of U.S. government agencies allowed to use those devices. An approval by the Pentagon is considered as the highest standards in security."

6. 2013: Smartphones and Handheld Devices for Defense and Homeland Security Strategies, Plans, Challenges & Opportunities Symposium:

a. “U.S. Coast Guard Smartphones Needs, Challenges & Opportunities” Rear Admiral Robert E. Day, Jr., Assistant Commandant for Command, Control, Communications, Computers & Information Technology, (C4IT) & Director, Coast Guard Cyber Command, Pre-Commissioning Detachment, U.S. Coast Guard.

b. “DoD Mobile Strategy” Mr. Mark Norton, Senior Engineer, Department of Defense, Office of the Chief Information Officer, Office of the Under Secretary of Defense (CIO/OSD).

c. “Update on Spectrum Sharing for Mobile Devices at the Tactical Edge” Mr. Julius Knapp, Chief Engineer, Office of Engineering and Technology, Federal Communications Commission (FCC).

d. “Secure Smartphone Computing, Needs and Opportunities for a Secure yet Mobile Platform” Mr. Keith Trippie, Executive Director, Enterprise System Development, Office of the Chief Information Officer, Department of Homeland Security (DHS).

e. “DISA’s Strategic Mobility Vision” Mr. Gregory Youst, Chief Mobility Engineer, Technology and Integration Division, Chief Technology Officer, Defense Information Systems Agency (DISA) (invited).

f. “Content-Based Mobile Edge Networking (CBMEN)” Dr. Keith Gremban, PhD., Program Manager, Content Based Mobile Edge Networking (CBMEN), Defense Advanced Research Project Agency (DARPA).

g. “Transformative Apps Program” Mr. Doran Michaels, Program Manager, Transformative Apps, DARPA.

h. “Windshear II Update” Mr. John-Isaac Clark, Chief Innovation Officer, Thermopylae Sciences & Technology & Mr. Lenwood Washington, Senior Systems Engineer, Mission Integration Directorate, Acquisition and Engineering, National Reconnaissance Office (NRO).

i. “Advancements in Mobile Devices for Chem-Bio Detection and Characterization” Dr. Calvin CHUE, PhD., Research Biologist, U.S. Army Research, Development and Engineering Command (RDECOM).



j. “ADAPT Unattended Ground Sensor Using Android Operating System and Original Design Manufacturers” Mr. Mark Rich, Program Manager, Strategic Technology Office, DARPA.

7. 2013: “The U.S. Department of Defense confirmed in a statement on Friday that Apple's iOS 6 mobile operating system is secure enough to connect to secure Pentagon networks.”

8. 2013: “Samsung's potential government deal signals new era for mobile security: Samsung may be ready to sign deals with the FBI and the U.S. Navy. Analysts say the news is proof that mobile in the enterprise has arrived. Samsung is close to inking a deal with the FBI and the U.S. Navy for mobile devices.”

9. 2013: “National Institute of Standards and Technology (NIST), which examines and tests mobile devices and technologies for security clearance, granted the Apple software FIPS 140-2 certification (Level 1) last Friday. This approves iPhones and iPads running the software in conjunction with the U.S. government's lowest level of national security clearance.”

10. 2013: “The U.S. Department of Defense announced today that it was further dropping its exclusive BlackBerry contract and opening all of its mobile communications networks to Apple, Google, and other device makers. ‘The Department of Defense is taking a leadership role in leveraging mobile device technology by ensuring its workforce is empowered with mobile devices,’ Defense Department Chief Information Officer Teri Takai said in a statement today.”

11. 2013: “Samsung recently received the nod from the Pentagon for any Samsung device protected by the Knox security software, which includes the Galaxy S4 and other compatible tablets.”

12. 2013: “For the first time, Apple's push into federal use opens up the U.S. government and military to competition for device procurement in the mobile space.”

13. 2014: “The mobile device management system—MDM—began operating Jan. 31 as a control system through which approved devices must operate to get access to Defense Department networks. The MDM enforces security policies by blocking or permitting certain functions on smartphones and tablets.”

14. 2014: “By opening its networks to Samsung and Apple devices, Defense Information Systems Agency (DISA) intends to broaden the variety of mobile computers that

troops and civilian Defense Department employees can use in the field, on bases, in offices and elsewhere to receive and send information and work almost anywhere at any time.”

15. 2014: “Samsung has announced that five of its Galaxy devices have been approved for the U.S government's Defense Information System Agency (DISA) products list. The devices include the Galaxy S4, Galaxy S4 Active, Galaxy Note 3, the Galaxy Note Pro 12.2 and the Galaxy Note 10.1 2014 Edition. All of them are using Android 4.4 (KitKat) along with Samsung's KNOX secure workspace platform, which includes system-level encryption for enterprise-based apps.”

16. 2014: “The United States Air Force is replacing 5000 legacy BlackBerry smartphones with Apple's iPhone, and eventually all of their BlackBerry users will have to make the changeover. The announcement, reported by Defense News, comes as the future of BlackBerry within the Department of Defense is debated, with the chips seeming to fall on the side of transitioning away from a network supporting a mish-mash of BlackBerry 6 and 7 devices to a mix of modern devices — though apparently without BlackBerry 10 in that mix.”

17. 2015: “Navy Plans for Android and iOS Devices. The Navy Enterprise Networks (NEN) Program Office is making progress on plans to transition to more modern mobile devices. Early users will be able to choose between the iPhone 5c and 5s, but the Navy wants to be as flexible as possible and allow users to pick the devices that will work best for them, and plans to approve a wider range of devices. Approval to use the iPhone 6 and iPad Air is expected in Jan. or Feb. 2015, and approval to use Samsung Android phones and tablets is expected in March.”

18. 2016: “This fiscal year Marines will receive Samsung smart phones that make calling for fire support easier, quicker and more accurate. The Target Handoff System Version 2, or THS V.2, is a portable system designed for use by dismounted Marines to locate targets, pinpoint global positioning coordinates and call for close air, artillery and naval fire support using secure digital communications.”

19. 2016: “Both the LG Electronics G5 and V10 received a security certification from the U.S. Defense Information Systems Agency, as well as a certification by the National Information Assurance Partnership, which administers independent tests to see if the devices are reliable and secure. The two newer LG smartphone models have joined the select list of official devices that can be used by Department of Defense employees, according to the handset manufacturer and a DOD website. LG's older models, the G3 and G4 also received DISA

certifications. The phones come equipped with LG's encryption technology from 2013, LG GATE. The advanced tech has secure email options, supports Virtual Private Network (VPN), and can remotely wipe the phone's memory."

20. 2016: "Use of Mobile Technology for Information Collection and Dissemination": A DACS Technology Assessment Report: The Data & Analysis Center for Software (DACS) was one of several United States Department of Defense (DoD) sponsored Information Analysis Centers (IACs), administered by the Defense Technical Information Center (DTIC). It was managed by the U.S. Air Force Research Laboratory (AFRL) and operated by Quanterion Solutions Inc. under a long-term DoD contract. The website is no longer available and was replaced by <https://www.csiac.org/> DACS Report Number 518055: Contract FA1500-10-D-0010; Prepared for the Defense Technical Information Center; Prepared By: Chet Hosmer, Chief Scientist; Carlton Jeffcoat, Vice President, Cyber Security Division; Matt Davis, Malware Analyst; Wetstone/Allen Corporation of America; 10400 Eaton Place; Fairfax, VA 22030; Thomas McGibbon, DACS Director; Quanterion Solutions Inc. 100 Seymour Road Utica, NY 13502. (Paragraphs a-f below were taken from the Report)

a. Mobile technology is increasingly being utilized as a tool for information dissemination and collection across the Government. The Department of Defense (DoD), Department of Homeland Security (DHS), Intelligence communities, and law enforcement are among those agencies utilizing mobile technology for information management. The primary mobile devices being utilized are the iPad®, iPhone®, Android™, and Windows Mobile™. The open architecture of these devices is advantageous for rapid application development and release.

b. New mobile technologies such as the iPhone®, iPad®, Android™ and similar devices have revolutionized the way information can be distributed. In the past, mobile devices such as Personal Data Assistants (PDAs) primarily focused on data storage and display. Today, an increasingly large number of devices are focusing not only on data storage and display, but also on communication and processing. As a result, organizations have begun leveraging mobile technology as a means of information dissemination. These organizations include, but are not limited to, Government organizations such as the Department of Defense (DoD), the United States Army, the

Department of Homeland Security (DHS), and a number of critical infrastructure organizations.

c. Significant advancements in mobile technology have occurred since September 11, 2001, both in the advancement of the devices and the infrastructures that support them. For example, mobile devices like the Android™ and iPad® can now operate equally and seamlessly via traditional cellular networks, as well as with infrastructure/ad hoc wireless networks.

d. The Defense Advanced Research Projects Agency (DARPA) has launched a program known as the Transformative Apps Program. The purpose of this program is to place the correct mobile applications into the hands of warfighters. To facilitate this, a military application store is being created to promote collaboration between developers and users in the field.

e. Another DoD initiative is Connecting Soldiers to Digital Applications (CSDA), sponsored by the Army Capabilities Integration Center (ARCIC) and the Army CIO/G6, with support from the Army Training and Doctrine Command (TRADOC) deputy commanding general for Initial Military Training, and other Army organizations. The purpose of this initiative is to determine the value of giving soldiers applications on mobile devices [ARMY]. During Phase One of the initiative the Army experimented with several types of smart phones to evaluate the effectiveness and usefulness of various mobile applications in the field. Devices tested included the Apple iPhone®, Google Android™ devices, and Microsoft Windows Mobile™ phones [C4ISR]. On these devices, applications were tested which covered a wide range of functions.

f. DoD is also starting to integrate chemical and biological sensors into mobile devices. Researchers from the University of California, San Diego have developed a miniature chemical sensor which can detect harmful gas in the air and automatically send the information about the type and transmitting range of the gas. The chemical sensor is a silicon chip with hundreds of independent miniature sensors. These can identify the molecule of specific toxic gas and then report on it.

21. The Bayh-Dole Act's coverage is not limited to procurement contracts governed by the Federal Acquisition Regulation but extends to all "funding agreements" for research and development. "Funding agreements" include contracts, grants, and cooperative agreements."

Only "subject inventions" are covered by the Bayh-Dole Act's provisions, so it is important to understand the definition of this term. "Subject invention" is "any invention of the contractor conceived or first actually reduced to practice in the performance of work under a funding agreement."

22. The statute is implemented in the "FAR" through the mandatory "Authorization and Consent" clause for solicitations and contracts:"

(a) The Government authorizes and consents to all use and manufacture, in performing this contract or any subcontract at any tier, of any invention described in and covered by a United States patent (1) embodied in the structure or composition of any article the delivery of which is accepted by the Government under this contract or (2) used in machinery, tools, or methods whose use necessarily results from compliance by the Contractor or a subcontractor with (i) specifications or written provisions forming a part of this contract or (ii) specific written instructions given by the Contracting Officer directing the manner of performance. The entire liability to the Government for infringement of a patent of the United States shall be determined solely by the provisions of the indemnity clause, if any, included in this contract or any subcontract hereunder (including any lower-tier subcontract), and the Government assumes liability for all other infringement to the extent of the authorization and consent herein above granted.

(b) The Contractor agrees to include, and require inclusion of, this clause, suitably modified to identify the parties, in all subcontracts at any tier for supplies or services (including construction, architect-engineer services, and materials, supplies, models, samples, and design or testing services expected to exceed the simplified acquisition threshold); however, omission of this clause from any subcontract, including those at or below the simplified acquisition threshold, does not affect this authorization and consent.

**CONTINUED GOVERNMENT INITIATIVES FOR A "NEW AND  
IMPROVED "CELL PHONE, SMARTPHONE, TABLET (I.E.,  
PLAINTIFF'S CMDC DEVICES).**

23. Plaintiff has included the alleged infringement of independent patent claims (13, 14, 15, 16, 17, 18, 19, & 20) of Plaintiff's '439 patent.

Patent #: 9,589,439; Independent Claim 13

"TOUGHBOOK 31" Laptop K-Max Self-flying Helicopter	Patent #: 9,589,439; Independent Claim 13
"TOUGHBOOK 31" Laptop Passport Systems Inc. Base Control Unit (BCU)	Patent #: 9,589,439; Independent Claim 13
Apple iPad Tablet Boeing MH-6 Little Bird Helicopter	Patent #: 9,589,439; Independent Claim 13
Navy Marine Corps Intranet (NMCI) Network - Apple iPad	Patent #: 9,589,439; Independent Claim 13
Smartphone-Based Rapid Diagnostic Tests	Patent #: 9,589,439; Independent Claim 13
Variable's "NODE+Oxa" for the Apple (iPhone) Smartphone	Patent #: 9,589,439; Independent Claim 13
"COINS" Nano-Embedded Sensors for Smartphones	Patent #: 9,589,439; Independent Claim 13
Samsung Galaxy s6 "BioPhone"	Patent #: 9,589,439; Independent Claim 13
"Biotouch" Samsung Galaxy s6	Patent #: 9,589,439; Independent Claim 13
PositiveID / "Firefly DX" Samsung Galaxy s6 Smartphone	Patent #: 9,589,439; Independent Claim 13

Patent #: 9,589,439; Independent Claim 14

"Cell-All": Samsung Galaxy s6	Patent #: 9,589,439; Independent Claim 14
Navy Marine Corps Intranet (NMCI) Network - Samsung Galaxy s6	Patent #: 9,589,439; Independent Claim 14



1"x2" Detection Device (DD) Samsung Galaxy s6 Smartphone	Patent #: 9,589,439; Independent Claim 14
--	---

NetS <sup>2</sup> SmartShield G500 Radiation Detector Samsung Galaxy s6 Smartphone	Patent #: 9,589,439; Independent Claim 14
--	---

"Kromek D3S-ID": A Standalone Isotope ID	Patent #: 9,589,439; Independent Claim 14
--	---

Patent #: 9,589,439; Independent Claim 15

MIT: "NFC" Samsung Galaxy s6 Smartphone Sensor	Patent #: 9,589,439; Independent Claim 15
--	---

Navy Marine Corps Intranet (NMCI) Network - Samsung Galaxy s6	Patent #: 9,589,439; Independent Claim 15
---	---

Patent #: 9,589,439; Independent Claim 16

NRL: SIN-VAPOR / Smartphone System	Patent #: 9,589,439; Independent Claim 16
------------------------------------	---

iPhone "Biodetector" Smartphone	Patent #: 9,589,439; Independent Claim 16
---------------------------------	---

FLIR: identiFINDER R300 / Smartphone System	Patent #: 9,589,439; Independent Claim 16
---	---

Patent #: 9,589,439; Independent Claim 17

"VOCKET System" / "Nett Warrior" Smartphone System	Patent #: 9,589,439; Independent Claim 17
--	---

GammaPix for Android Smartphones	Patent #: 9,589,439; Independent Claim 17
----------------------------------	---

"Biotouch System" / "Nett Warrior" Smartphone System	Patent #: 9,589,439; Independent Claim 17
--	---

MultiRae Pro Wireless Portable Multi Threat Radiation and Chemical Detector	Patent #: 9,589,439; Independent Claim 17
---	---

Patent #: 9,589,439; Independent Claim 19

EAGER: Mobile-Phone Based Single Molecule Imaging for DNA	Patent #: 9,589,439; Independent Claim 19
INSPIRE Track 2: Public Health Nanotechnology and Mobility (PHeNoM)	Patent #: 9,589,439; Independent Claim 19
PFI:BIC Human-Centered Smart-Integration of Mobile Imaging and Sensing	Patent #: 9,589,439; Independent Claim 19
EFRI-BioFlex: Cellphone-Based Digital Immunoassay Platform	Patent #: 9,589,439; Independent Claim 19
"Multimode Smartphone Biosensor"	Patent #: 9,589,439; Independent Claim 19
EAGER: Lab-in-a-Smartphone	Patent #: 9,589,439; Independent Claim 19
PFI-BIC "Pathtracker: Smartphone-based for Mobile Infectious Disease Detection	Patent #: 9,589,439; Independent Claim 19
I-Corps: Ultra-Sensitive Lateral Flow Reporters / Lab-on-Phone Platform	Patent #: 9,589,439; Independent Claim 19
Smartphone (iPhone) Microscope	Patent #: 9,589,439; Independent Claim 19
Smartphone (iPhone) Biosensor "Cradle"	Patent #: 9,589,439; Independent Claim 19
AOptix Stratus MX Peripheral for the Apple (iPhone) Smartphone	Patent #: 9,589,439; Independent Claim 19
PositiveID - Boeing / M-Band Apple (iPhone) Smartphone	Patent #: 9,589,439; Independent Claim 19
Samsung Galaxy s6 "Microscope" Smartphone	Patent #: 9,589,439; Independent Claim 19



Patent #: 9,589,439; Independent Claim 20

"Cell-All": Apple iPhone	Patent #: 9,589,439; Independent Claim 20
"Kromek D3S-NET": Apple iPhone	Patent #: 9,589,439; Independent Claim 20
Biomeme "two3" Mobile Thermocycler: Apple iPhone	Patent #: 9,589,439; Independent Claim 20
Smartphone-operated "LAMP box": Apple iPhone	Patent #: 9,589,439; Independent Claim 20
Alluviam LLC HazMasterG3: Apple iPhone	Patent #: 9,589,439; Independent Claim 20
FePhone Point-of-Care: Apple iPhone	Patent #: 9,589,439; Independent Claim 20
NutriPhone Lab-on-a-Chip: Apple iPhone	Patent #: 9,589,439; Independent Claim 20
FeverPhone: Apple iPhone	Patent #: 9,589,439; Independent Claim 20
Solar Thermal PCR Test: Apple iPhone	Patent #: 9,589,439; Independent Claim 20
Lab-on-a-Drone: Apple iPhone	Patent #: 9,589,439; Independent Claim 20

### **PLAINTIFF'S PROGRESSIVE SETTLEMENT OFFER**

In the parties' e-mail correspondence, (**Exhibit D**), Plaintiff presented to the Government a progressive settlement offer. The District Court has in place incentives to encourage Defendant's not to engage in stall tactics, such as the one the Government has presented in its

proposed scheduling order, by issuing preliminary injunctive relief and/or awarding triple damages for willful infringement.

The Court of Federal Claims is barred from granting preliminary injunctive relief and/or awarding triple damages for willful infringement. This Court is limited to awarding a reasonable royalty. Plaintiff therefore introduced to the Government a progressive settlement offer that is described as follows:

“Plaintiff believes this case should be settled between the Parties. Plaintiff also believes the Defendant should be held accountable if he/she continues to force needless, unnecessary, and redundant litigation. Plaintiff is proposing a settlement of one billion dollars tax free or one billion, four hundred million dollars taxable.

Since 2002, DHS has awarded nearly \$54 billion in preparedness grants to strengthen our nation’s ability to prevent, protect against, mitigate, respond to and recover from terrorist attacks, major disasters, and other emergencies in support of the National Preparedness Goal and the National Preparedness System. Plaintiff started his projects of terrorist prevention in 2002.

To this day, Plaintiff has received “zero” dollars for what could be consider the most effective means of preventing, protecting against, mitigating, responding to and recovering from terrorist attacks this Nation has seen. Equipping 240M participants (to form a network of ubiquitous sensing) with the ability to detect for CBRNE-H is without parallel. Calculation: \$54 billion dollars divided by 18 years equals \$3 billion dollars per/year. For Plaintiff’s contribution to our Nation’s security, Plaintiff is willing to settle for \$1 billion tax-free.

Provided the DHS was appropriated \$8 billion dollars for SBI-Net and \$3 billion dollars for Bio-Watch 3, I’m sure the Government can see the value of a non-exclusive license for the rights to manufacture and use technology to prevent, protect against, mitigate, respond to and recover from terrorist attacks on a mass scale for only \$1 billion dollars tax-free.

To settle now, before claim construction is instituted, one billion dollars tax free or one billion, four hundred million dollars taxable. If claim construction is instituted, add another one billion dollars tax free or one billion, four hundred million dollars taxable. If during claim construction Plaintiff has to relitigate (construe) any material that has been

previously litigated, add another one billion dollars tax free or one billion, four hundred million dollars taxable.

If patent infringement analysis is instituted, add another one billion dollars tax free or one billion, four hundred million dollars taxable. If Plaintiff has to defend against unsubstantial limitations beyond that of a communication/monitoring device comprising a central processing unit capable of processing instructions to detect for CBRNE, i.e., biometric authentication; disabling lock after multiple fail attempts to open; radio frequency near-field communication; C/B medical detection and diagnosis; locking and unlocking of doors; control the operating systems of vehicles; stall, stop and slowdown vehicles; operate unmanned aerial, sea and land vehicles; or the inclusion of an enhanced GPS location and tracking system, add another one billion dollars tax free or one billion, four hundred million dollars taxable per occurrence.

If patent validity is instituted, add another one billion dollars tax free or one billion, four hundred million dollars taxable. If Plaintiff again has to defend against patents that do not antedate Plaintiff's priority date for his patents, add another one billion dollars tax free or one billion, four hundred million dollars taxable per occurrence. If Plaintiff has to defend against patents that has already been presented in the prosecution of any of Plaintiff's patents, add another one billion dollars tax free or one billion, four hundred million dollars taxable per occurrence. If Plaintiff has to defend against rejections (i.e., challenging the patents' validity) that are not presented on the heightened standard of "clear and convincing evidence", add another one billion dollars tax free or one billion, four hundred million dollars taxable per occurrence."

In the e-mail correspondence, Plaintiff also warned the Government not to offer Apple, Samsung, and LG shelter away from litigating in the District Courts. According to the Government, "Apple, Samsung, and LG may have an interest in establishing their respective rights to manufacture, use, and sell the accused commercially available consumer electronics devices free from claims of infringement, as illustrated by Plaintiff's suits filed in the District of South Carolina." (Dkt 216; Case No. 1:13-cv-00307-EG).

"If you establish back to this case, Apple, Samsung, and LG as third-party government contractors to the Cell-All initiative, my settlement terms will change

enormously... Establishing Apple, Samsung, and LG as third-party government contractors to the Cell-All initiative means I could possibly be deprived of having my case(s) heard by a jury; deprived of a preliminary injunction; deprived of an SEC mandatory reporting of a lawsuit that is equivalent to 10% or more of a company's assets; deprived of an SEC mandatory reserve requirement imposed on the companies to cover estimated damages (**Exhibit D**) resulting from a lawsuit; deprived of triple damages for willful infringement; and, deprived of litigating Plaintiff's Antitrust Law Violations case."

### **CLAIM CONSTRUCTION**

Plaintiff also explained to the Government that the Plaintiff has undergone "claim construction" during a PTAB instituted *inter partes review* (IPR) (**Exhibit D**) that was petitioned by Government agencies (i.e., Defendants the DOJ & DHS) who were not "persons" authorized to petition the PTAB to institute a trial to invalidate a Patent Owner's patents or patent claims *Return Mail v. The United States*. PTAB Final Written Decision: "Claim Construction in an *inter partes review*, we interpret claim terms in unexpired patents according to their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1276–79 (Fed. Cir. 2015)." "[i]n the Decision to Institute, we construed certain claim terms... Claim Term Construction: 'communication device' (claim 81) construed to mean the same as 'monitoring equipment' Dec. to Inst. 11–16. No party challenges these constructions."

Collateral estoppel (**Exhibit D**) applies when the following five elements are satisfied: "(1) the identical issues were presented in a prior proceeding; (2) there was a full and fair opportunity to litigate the issues in the prior proceeding; (3) the issues in the prior litigation were a critical and necessary part of the prior determination; (4) the parties in the two proceedings were identical; and (5) the issues were actually litigated in the prior proceeding." *Pearce v. Sandler*, 219 So.3d 961, 965 (Fla. 3d DCA 2017) quoting *Topps v. State*, 865 So.2d 1253, 1255 (Fla. 2004). When these elements are satisfied, "[c]ollateral estoppel precludes re-litigating an issue where the same issue has been fully litigated by the parties or their privies, and a final decision has been rendered by a court." *Id.* quoting *Mtge. Elec. Registration Sys., Inc. v. Badra*, 991 So.2d 1037, 1039 (Fla. 4th DCA 2008).

Plaintiff is asking this Court to accept in good faith Plaintiff's progressive settlement schedule as fair to both parties in the ongoing upcoming proceedings.

**PLAINTIFF OBJECTS TO ANY FURTHER ACTION BY THE  
GOVERNMENT ON CHALLENGING THE VALIDITY OF PLAINTIFF'S  
PATENTS**

The AIA of 2011 created... post-grant patent review proceedings... available to any "person" who is not the patent owner... "if the U.S is sued in a patent dispute, can it bring one of these AIA challenges? On June 10, 2019, the Supreme Court in *Return Mail Inc. v. United States Postal Service*, holding that the answer is no—the U.S. Government is not a "person" with standing to bring petitions for AIA post-grant review proceedings."

Three years after the AIA of 2011 the Government filed on April 30, 2014, a Petition for *Inter Partes Review* (IPR): *United States Department of Homeland Security / Petitioner, V. Larry Golden / Patent Owner*; Case IPR2014-00714; U.S. Patent No. RE043,990; filed by Lavanya Ratnam, Department of Homeland Security (DHS), and joined by Kirby Wing-Kay Lee, Department of Justice representing the United States.

It is the belief of Plaintiff, the Government knew, or should have known, it was not a "person" for purposes of petitioning the PTAB to institute patent validity. Therefore, the timing and decision of *Return Mail* did not change the "law" that was established in year 2011. The decision in *Return Mail* only upheld a "law" already in existence at the time of the Government's filing in year 2014. Plaintiff spent eighteen months trying to defend against a frivolous and bad faith *inter partes review* (IPR).

It is further the belief of Plaintiff, the DOJ and DHS deliberately submitted prior art references in its petition for *inter partes review* that does not antedate the Plaintiff's '990 patent asserted in the petition. The PTAB was given notice that the prior art references of Astrin, Breed, and Mostov, asserted in the IPR, does not antedate Plaintiff's RE43990 patent. The notice can be found at Case 1:13-cv-00307-EGB Document 48 Filed 07/30/14 Page 4 of 15. PATENT OWNER'S PRELIMINARY RESPONSE. "Pursuant to 35 U.S.C. § 313 and 37 C.F.R. § 42.107:

"the Patent Owner hereby provides a Preliminary Response to the April 30, 2014 Petition for *Inter Partes Review* ("Pet.") ... I. Inter Partes Review should not be instituted based

on anticipation by Astrin, Mostov and Breed because neither antedates or anticipates any of the challenged claims 11, 74 and 81 of Golden's '990 patent:"

The second notice was during the entire IPR review. The last notice I submitted to the PTAB as proof the prior art references of Astrin, Breed, and Mostov, asserted in the IPR, does not antedate Plaintiff's RE43990 patent was in Plaintiff's "Request for Rehearing" filed on October 24, 2015 with the PTAB Case IPR2014-00714 Patent RE43,990. The PTAB finally recognized in the Final Decision that the two patents of Astrin and Breed, instituted at the start of the *inter partes* review, did not antedate Plaintiff's '990 patent. But, without notice and without a chance to defend Plaintiff's patent and patent claims, the PTAB reintroduced the Mostov patent because the PTAB believed the Mostov patent antedated the Plaintiff's '990 patent.

**Submitted with Plaintiff's PTAB Request for Rehearing**

Reference	Filing Date	Publication Date	Basis for anticipation
U.S. Patent Application Publication No. 2006/0250235 ("Astrin")		11/09/2006	102(b)
U.S. Patent Application Publication No. 2006/0181413 ("Mostov")		08/17/2006	102(b)
U.S. Patent No. 7,961,094 ("Breed")	11/29/2007		102(e)
<i>Petitioner's First patent application No. 11/397,118 was filed with the USPTO. '990 patent claims priority</i>	<i>04/05/2006</i>		
U.S. Patent provisional filing date is 01/28/05. Appl. No. 11/343,560; Patent No. 7,990,270 ("Mostov")	01/28/2005		102(e)
<i>Petitioner's Disclosure Document filed with USPTO. Disclosure Doc. No. 565732</i>	<i>11/26/2004</i>		

Mostov's patent provisional filing date is January 28, 2005. The Patent Owner's "Disclosure Document" filing date is November 26, 2004. Therefore, any subject matter Mostov has outlined in his claims, according to the Federal Circuit decision above, is anticipated by the Patent Owner's "Disclosure Document" that antedates Mostov's patent provisional filing date. (A copy of the "Disclosure Document" was submitted to this Court and the USPTO for the benefit of the Patent Owner that displays a USPTO stamped filing date of November 26, 2004 and a stamped document no. of 565732 used for reference.)

The Department of Homeland Security's Lavanya Ratnam asserted in the petition for Inter Partes Review: the three (3) prior art references of Astrin, Mostov and Breed; eighteen (18) prior art publications; and, one Expert Declaration. 2131 Anticipation 35 U.S.C. 102 "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, (Fed. Cir. 1987)

The DHS raised a 101-patentability objection; a 102-anticipation objection; a 112-lack of written description objection; and, a 120-priority objection in the IPR petition: Page 2 of the IPR petition, "[a]t least claims 11, 74 and 81 of the '990 patent is not entitled to the benefit of the April 5, 2006 filing date pursuant to 35 U.S.C. § 120... page 3 "no description of this structure... is found anywhere in the '118 application". If Plaintiff decides not to amend to overcome the 101, 112, and 120 objections, the PTAB invalidate the challenged claims; remove the 101, 112, and 120 objections and the PTAB invalidate the claims for "broadening". 35 U.S.C. § 311(b) Scope. "A petitioner [DHS] in an *inter partes review* may request to cancel as unpatentable 1 or more claims of a patent only on a ground that could be raised under section 102 or 103".

Plaintiff filed substitute independent claims 154, 155, & 156. Plaintiff sent the new claims over to the USPTO to be examined against the DOJ and the DHS three (3) prior art patents; eighteen (18) prior art publications; and, one Expert Declaration asserted in the IPR. The examiner stated the prior art did not cover claims 154, 155, & 156 as a whole. The PTAB rejected the USPTO's findings and denied Plaintiff's substitute claims. Plaintiff loss three original independent claims of the '990 patent; sixty-nine dependent claims that depend on the original independent claims (11, 74, & 81) of the '990 patent; and three substitute independent claims (154, 155, & 156).

As a general rule, a litigant is deemed to have perpetrated a fraud on the court when "it can be demonstrated, clearly and convincingly, that a party has "purposely set in motion some unconscionable scheme calculated to interfere with the judicial system's ability to adjudicate impartially a matter by improperly influencing the [trier of fact] or unfairly hampering the presentation of the opposing party's claim or defense." *Cox*, 706 So. 2d at 46 (quoting *Aoude*, 892 F. 2d at 1118).

The IPR was instituted on the '990 patent. The '990 patent has the same claimed invention(s); same subject matter specifications as the patents-in-suit of this case i.e., the '497, '752, '189, '439, and '287 patents.

Plaintiff has included as **Exhibit E**, a list (history for all of Plaintiff's patents asserted in this Case) of the cited references for Patent No. 10,163,287 ('287 patent). Plaintiff has also included 59 other references "cited by applicant" that the Plaintiff disclosed to the USPTO for review in Patent No. 10,163,287 ('287 patent).

Plaintiff's patent specifications, that are the same for all of Plaintiff's patents, has undergone normal prosecution/examination; a vigorous re-issue prosecution/examination; an *inter partes review* (IPR); and, just recently in patent application 16/350,683, a challenge stemming from Apple's inventor Gloria Lin relating to a list of Apple references Plaintiff disclosed to the USPTO, in a 2010 letter addressed to Bruce Sewell, SVP & General Counsel of Apple Inc. (**Exhibit E**)

## CONCLUSION

The International Trade Commission's Court can determine patent infringement or non-infringement in 12 to 18 months. The average time for this Court is 2 to 3 years. In less than 2 months this case will have been opened for 8 years. The only thing the Government needs to do now is to present its case of non-infringement or settle.

Respectfully submitted,

\_\_\_\_\_

Larry Golden, Plaintiff, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607


atpg-tech@charter.net



**CERTIFICATE OF SERVICE**

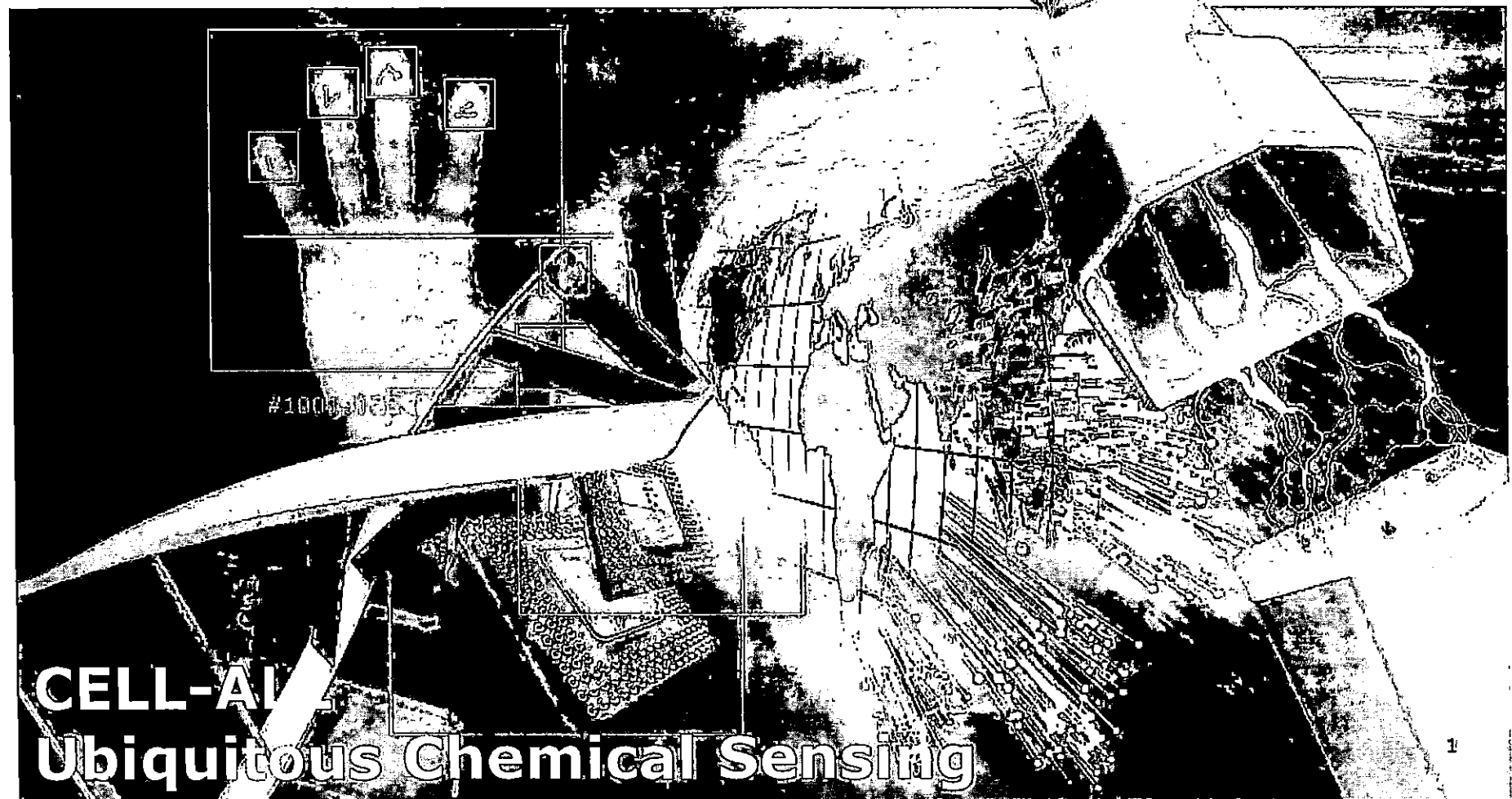
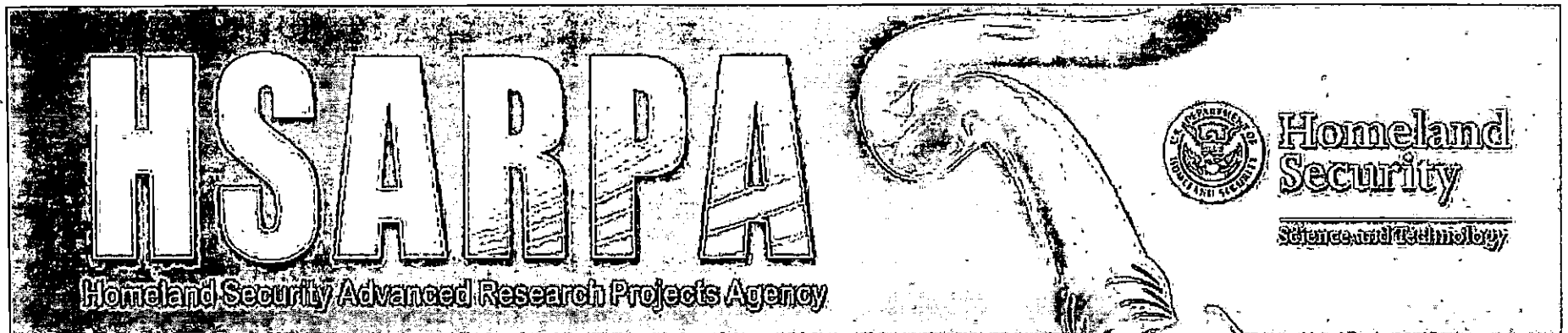
The undersigned hereby certifies that on this 27th day of March, 2021, a true and correct copy of the foregoing PLAINTIFF'S STATUS REPORT AND LEAVE OF THE COURT TO FILE A MOTION FOR DEFAULT JUDGEMENT was served upon the following defendant by Priority "Express" Mail:

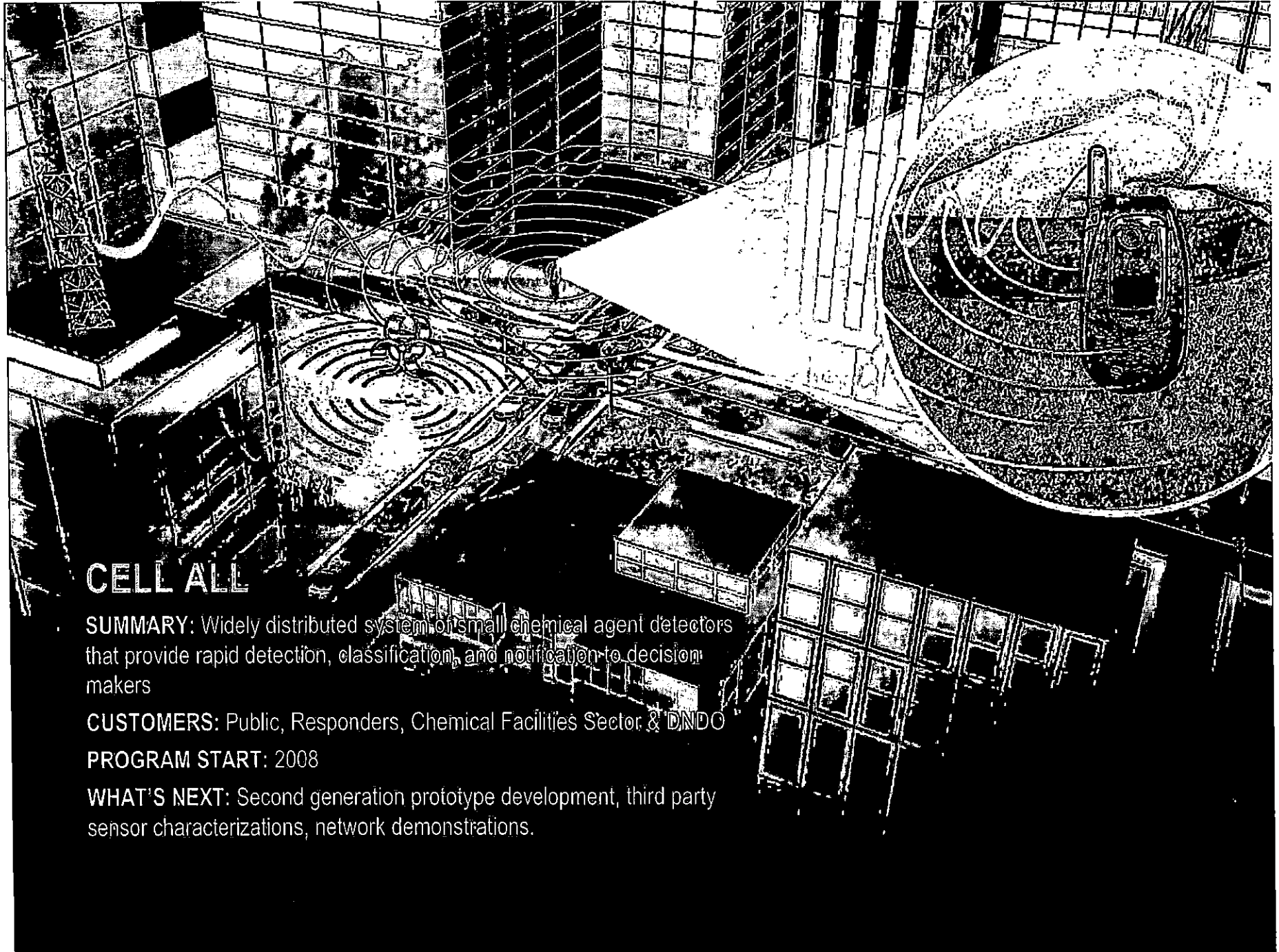
Grant D. Johnson  
Trial Attorney  
Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
Grant.D.Johnson@usdoj.gov  
202-305-2513

s/   
Larry Golden, Pro Se  
740 Woodruff Rd., #1102  
Greenville, South Carolina 29607  
atpg-tech@charter.net

# *Exhibit*

9





## CELL ALL

**SUMMARY:** Widely distributed system of small chemical agent detectors that provide rapid detection, classification, and notification to decision makers

**CUSTOMERS:** Public, Responders, Chemical Facilities Sector & DNDO

**PROGRAM START:** 2008

**WHAT'S NEXT:** Second generation prototype development, third party sensor characterizations, network demonstrations.

# Cell-All Goals

---

## Homeland Security Goals (QHSR)

### Mission 1: Preventing Terrorism and Enhancing Security

- Goal 1.1: Prevent Terrorist Attacks
- Goal 1.2: Prevent the Unauthorized Acquisition or Use of Chemical, Biological, Radiological, and Nuclear Materials and Capabilities

### Mission 5: Ensuring Resilience to Disasters

- Goal 5.1: Mitigate Hazards
- Goal 5.2: Enhance Preparedness
- Goal 5.3: Ensure Effective Emergency Response
- Goal 5.4: Rapid Recovery

## S&T Goals

- Rapidly develop and deliver knowledge, analysis, and innovative solutions that advance the mission of the Department

## HSARPA Goals

- Proof of concept technology development and demonstration
- Potential for significant gains in technical capability



Homeland  
Security

## Motivations to Improve Detection

---

Large, expensive and stationary systems represent state of the art for chemical agent detection

A variety of less expensive handheld systems are available as separate systems

Geographic coverage is limited to specific areas for each deployment

Sampling may not reflect the environment where people are actually located



Homeland  
Security

# Approach

---

## Create a large and dynamic sensing system

- Miniaturized and effective sensing capability
- Integrate low-cost sensing into common devices
  - Sensing becomes part of the environment
- Harvest the benefits of network effects and crowd sourcing
- Privacy Protection for individuals
- Integrate with 261 million cell phones now used in the U.S.
- Leverage billions of dollars spent each year in sensor, carrier network and cell phone development

Gain earlier indications and warning for hazardous chemical events



Homeland  
Security

# Technical Approach

---

## Embedded Miniature Sensors

- Sample collection
- Reusable devices with lifetimes that equal that of the host device
- Address sensor sensitivity & selectivity in the environment
- Prototype concepts for integrated sensing
- Methods for read/report of sensor information

## Sensing Network to Significantly Expand Coverage

- Investigate sensor performance in a large scale networks
- Concepts of Operation for ubiquitous sensing
- Modeling large scale system characteristics and response



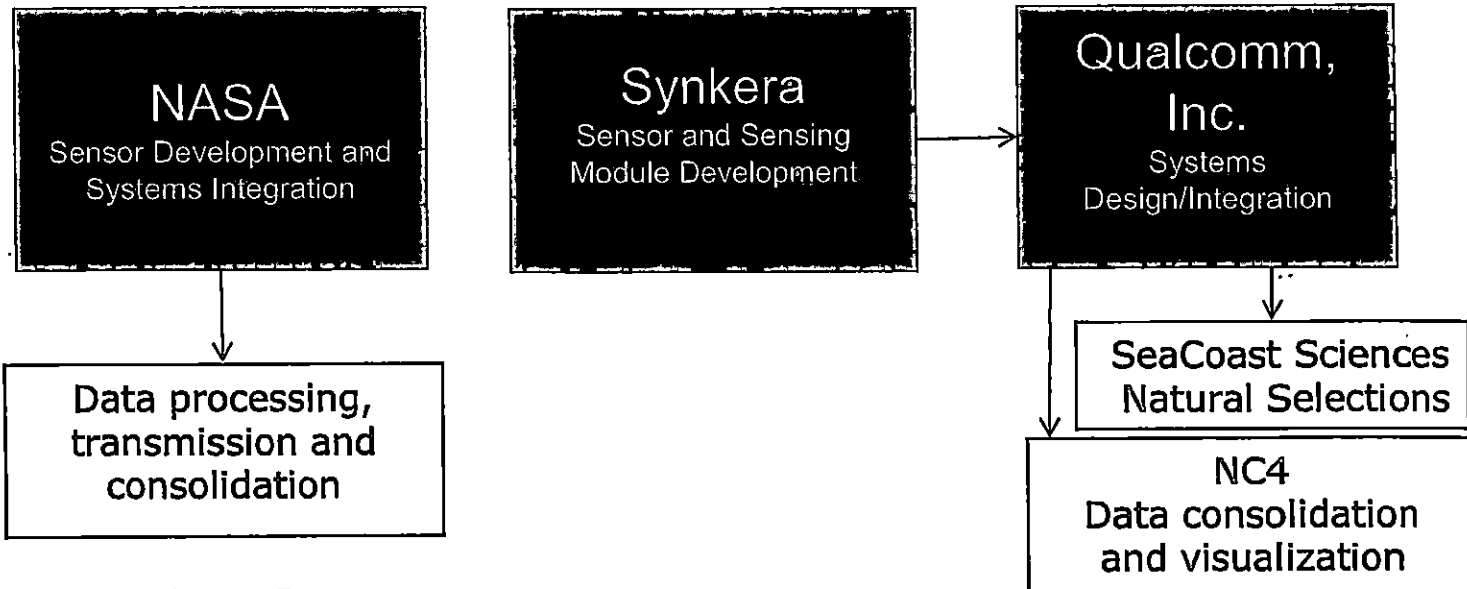
Homeland  
Security



# CellAll Team

---

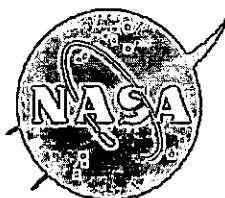
HSARPA  
Concept, architectural guidance & funding



Homeland  
Security

# Performers

---



## NASA Ames Research Center

Developed a world smallest and ultra low power nanosensor array module with sensors, a sampling device and a data acquisition board all-in-one (a stamp size) integrated with an iPhone and an app for data processing and transmission



## Qualcomm

State-of-the-art miniaturized detection system integrated into Android cell phones



## Synkera

Sensor & Module Developer



Homeland  
Security

# Phase 1 – Proof of Concepts

---

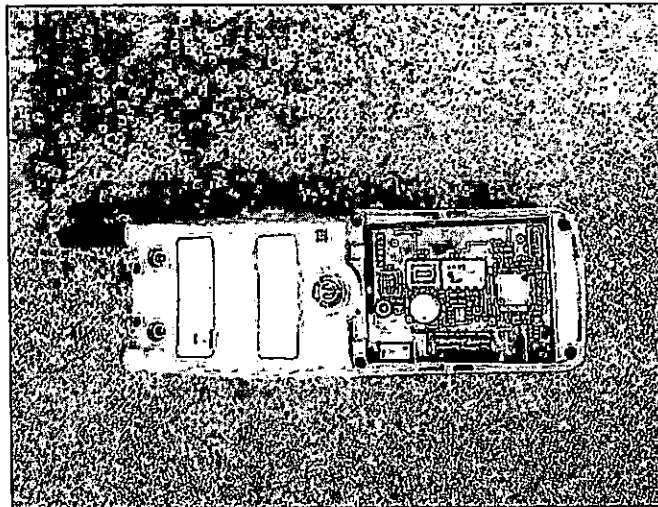
- Establish miniature sensor efficacy
- Discover limitations for cell phone integration
- Develop first generation prototypes
- Proof of concept demonstrations
  - NASA – Leveraging nanosensor work for space missions to further miniaturizing the space qualified integrated sensing system for detection of toxics and CWAs using smartphones.
  - Synkera – Leveraging SBIR funded development of miniature sensors.
  - Qualcomm – Using an existing hardware platform to integrate an existing sensor and demonstrate its ability to sense a defined set of agents



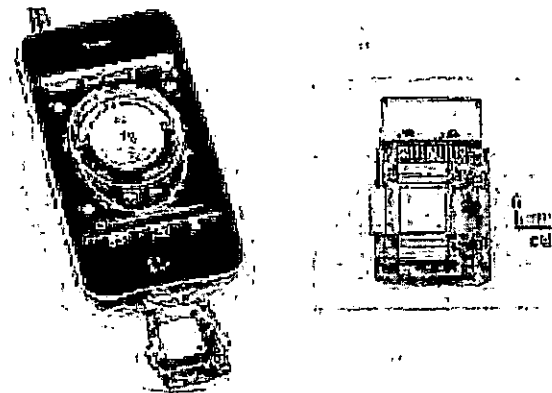
Homeland  
Security

# Phase I Prototypes

## Qualcomm FFA



## NASA ARC nanosensor module for iPhone integration



## iPhone Specifications



Homeland  
Security

## Phase II Prototypes

---

- Achieve a greater number of total prototype devices at a reasonable unit cost
- Sensor data transmission via 3g and/or Wi-Fi
- Multiple sensors network for chemical profiling
- Decouple the chemical sensor from the phone.
- Multiple sensor units per phone are possible
- Bluetooth/Proprietary Interfaces
- Standardize the sensor platform
- Increase opportunities for participation



Homeland  
Security

# Summer 2011 Demonstrations

---

- LAFD, Frank Hotchkins Memorial Training Center
  - Carbon Monoxide
  - Personal Protection Scenario
  - Audio Alarm
  - In Case of Emergency (ICE) Alerts
  
- FEMA, Center for Domestic Preparedness
  - Toxic Chemical Agents
  - Hazardous Materials Response Team Scenario
  - Network response
  - Geographic-based visualization



Homeland  
Security

# *Exhibit*

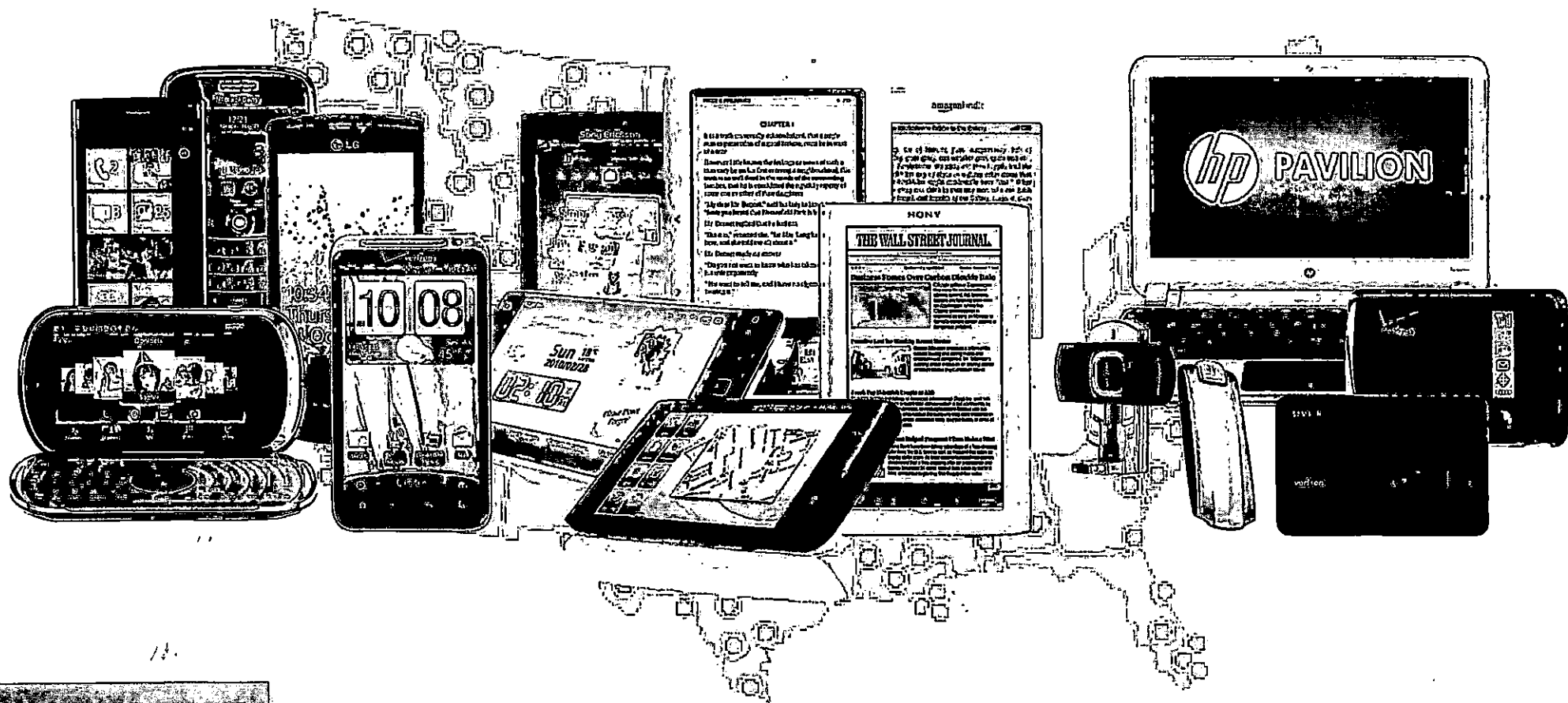
10

**QUALCOMM®**



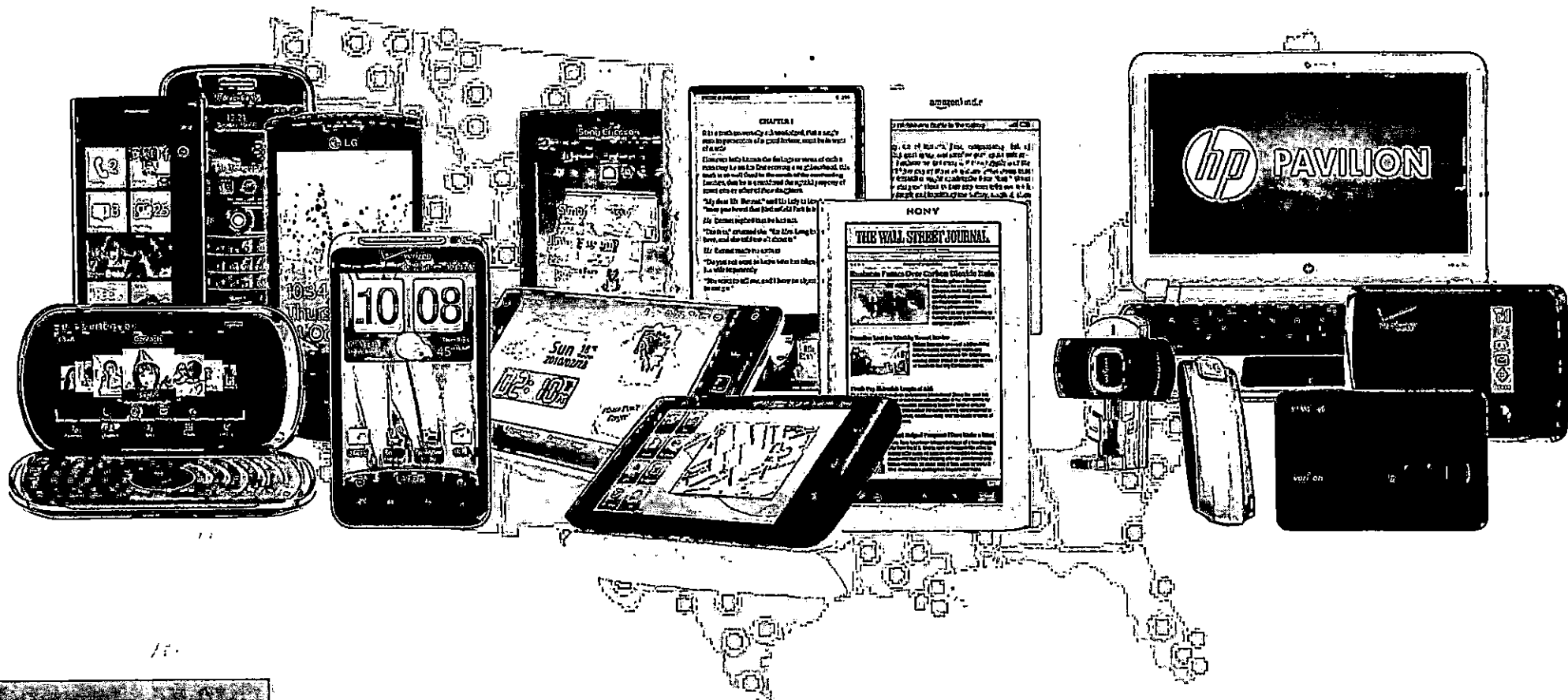
DHS asked, "what if..."

...we wanted to provide high impact ubiquitous technology for CBRNE sensing?

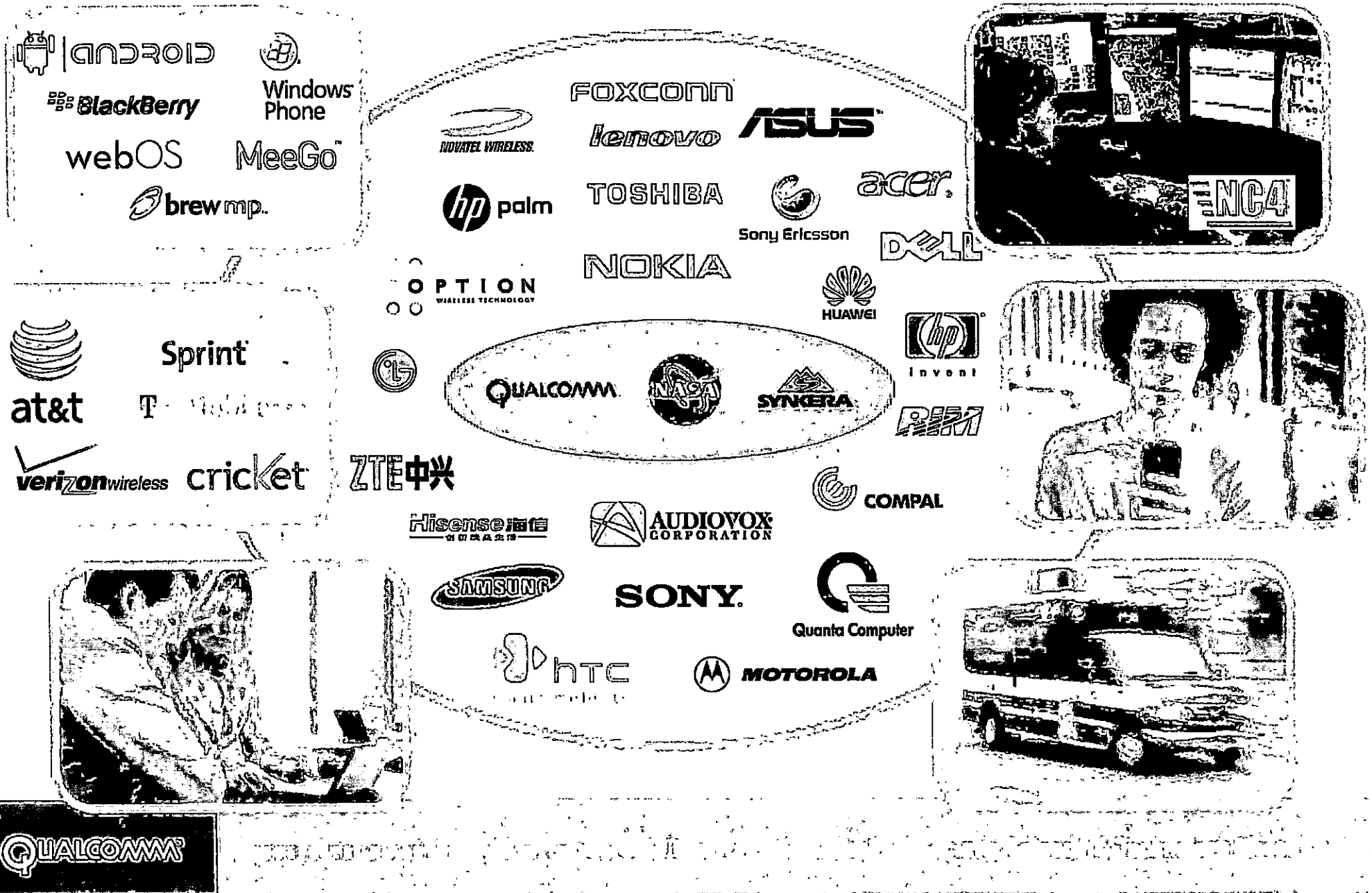


# DHS asked, "what if..."

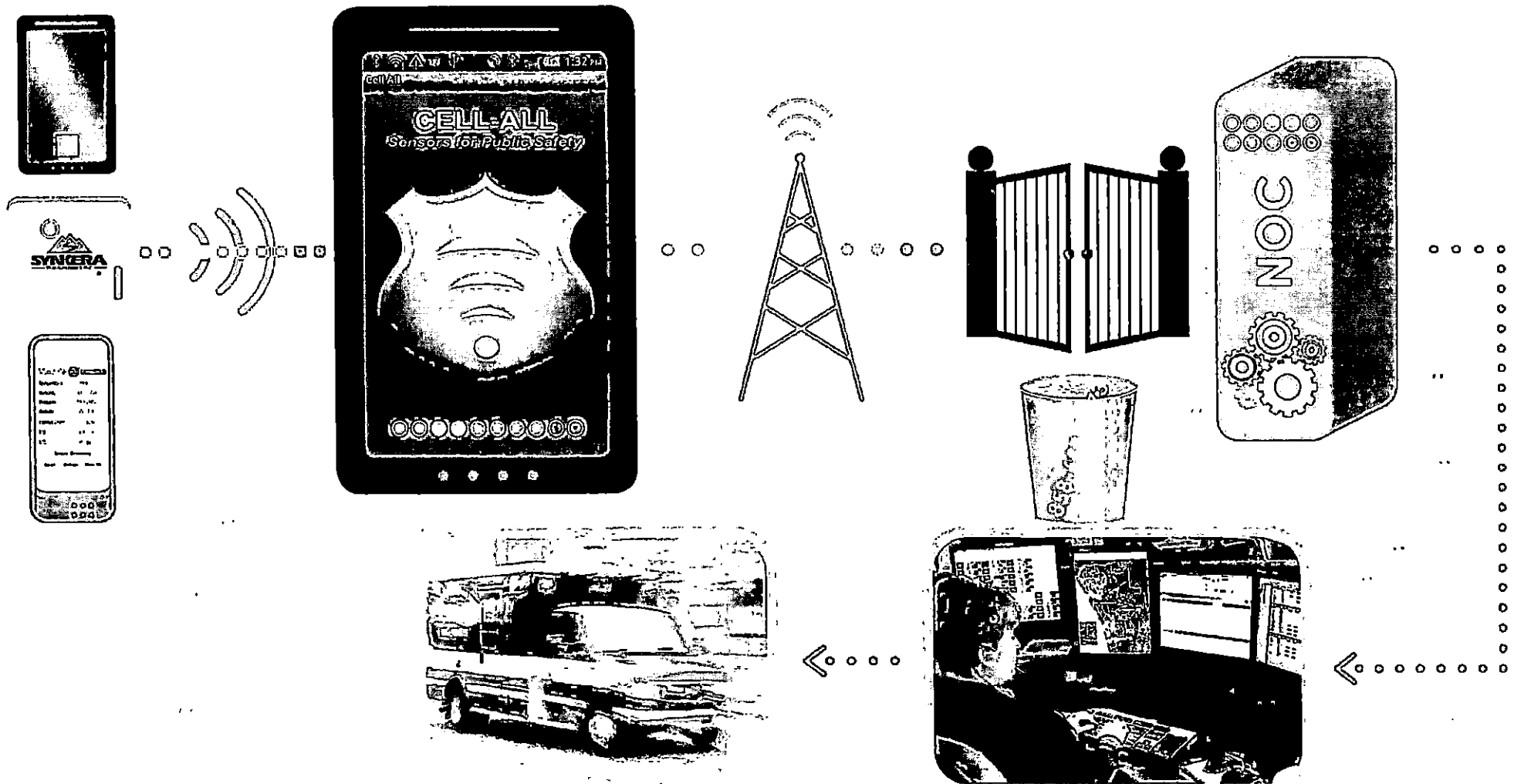
## Answer: Use commercial cellular phone ecosystem and commercial networks



# Who are the necessary stakeholders?



## How does it work?



# What's left to do?



## FIRST RESPONSE COMMUNITY

- Seamless integration to their workflow
- Training in the use of Cell-All

## BUSINESS

- How to make it attractive for all stakeholders

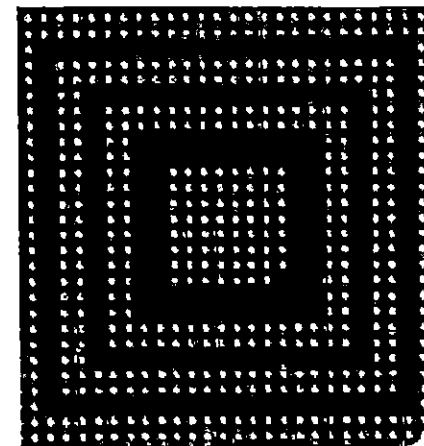


## SYSTEM

- First responder and user trials
- Performance and scalability
- Enhance security for commercial use
- Refine algorithm

## SENSORS

- Manufacturing Volumes
- Reproducibility
- Power
- Integration



# *Exhibit*

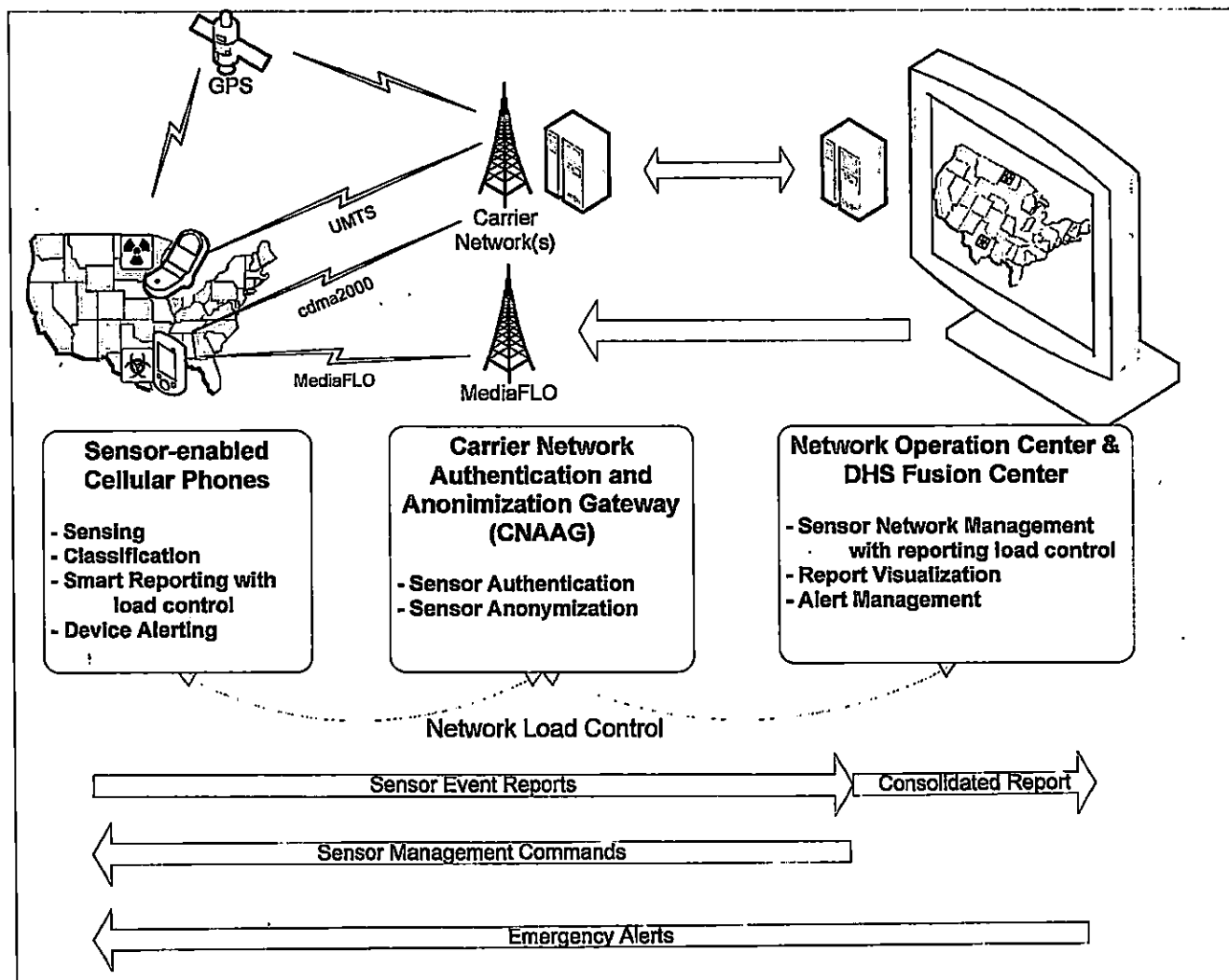
11



UNCLASSIFIED

QUALCOMM Government Technologies

## Network control and architecture



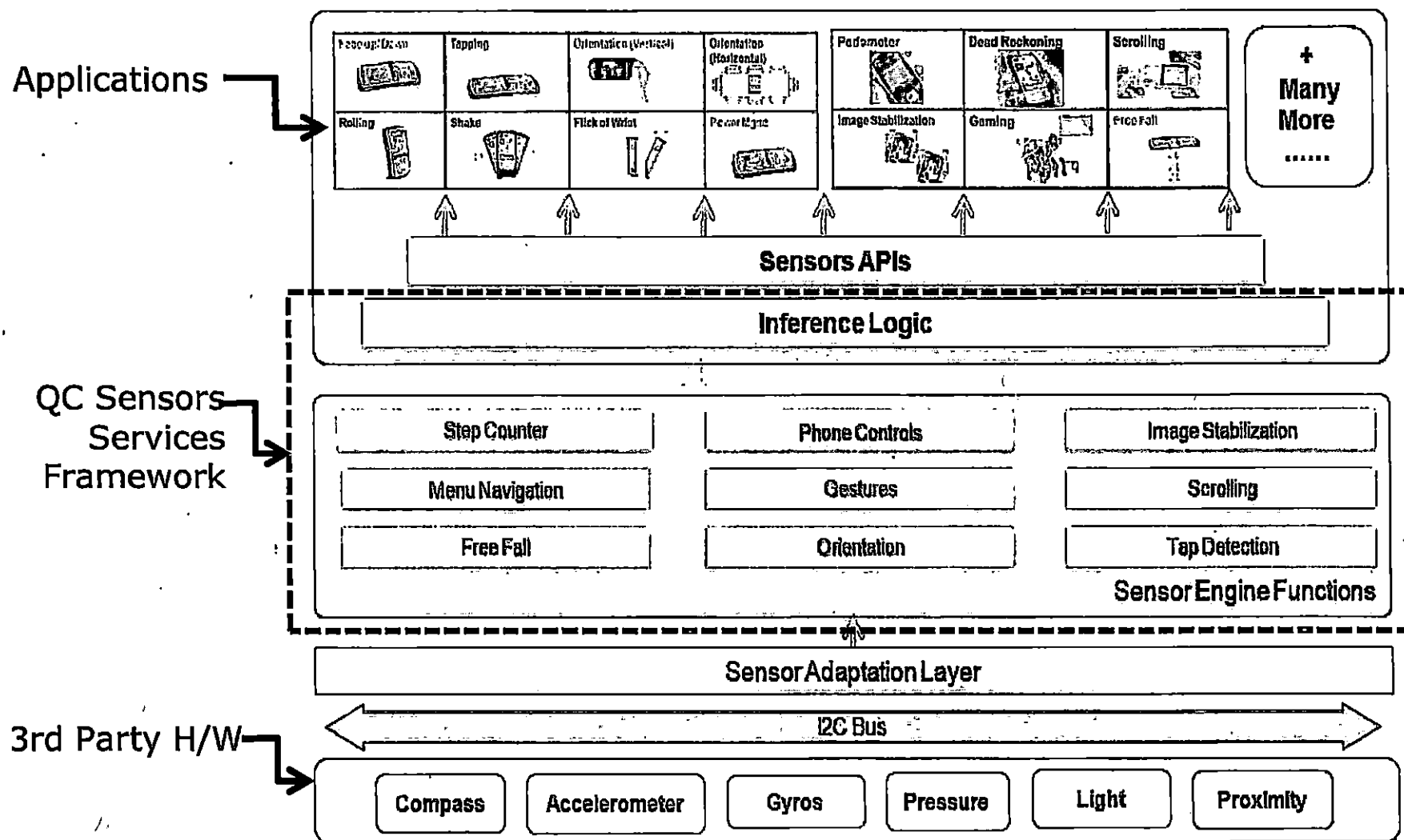
UNCLASSIFIED



UNCLASSIFIED

QUALCOMM Government Technologies

## Sensors Services Framework – Approach



UNCLASSIFIED





UNCLASSIFIED

QUALCOMM Government Technologies

## Cell Phone Environment

- Handsets are very price sensitive
- Components must be small and thin
- Battery life is a key benchmarks and more is better
- Short development time
- Short life cycle
- No time for redesigns
- Must be adaptable to standard manufacturing processes
- Temperatures/humidity/pressure fluctuate (Polar to Equator externally)
- RF interference issues
- Applications must be thin
- Algorithms must be efficient
- False positives will make this fail

UNCLASSIFIED



UNCLASSIFIED

QUALCOMM Government Technologies

## More details

- **Cost**

- Features like this usually require component cost of <\$1.00 (including support sensors for humidity, pressure and temperature if necessary)
- Studies indicate
  - Consumers might be willing to pay the additional cost of \$1.00.
  - A personal sensing application for CO may improve up take
  - False positives would kill feature quickly
- The cost associated with the manufacturing process is equally important
  - OEMs cannot be expected to calibrate (self calibration)
  - Must use a standard operating system

UNCLASSIFIED



UNCLASSIFIED

QUALCOMM Government Technologies

## More details

- Digital Interfaces

- UART (up to 4Mbps)

- Two wire interface (Transmit/Receive)
    - Supporting asynchronous data

- I2C (typically used for sensors)

- Used for command and control of devices such as the camera
    - Two wire Master/Slave type bus
    - Clock line and data line
    - Supports 1 Master and multiple Slaves
    - Generally supports 100KHz and 400KHz operation on the bus

- Analog

- Some handsets support this
    - Typically used for temperature
    - May offer integration advantages

UNCLASSIFIED



UNCLASSIFIED

QUALCOMM Government Technologies

## More details

- **Manufacturing Consideration**
  - Manufacturing temperatures as high as 260° C possible
    - A flex circuit or socket approach may be necessary
  - Size
    - 3-15 sensors on a <6x6x2mm optimally 2x2x1mm
    - Including components necessary for support (fans, vents, filters, dwell)
  - Packaging – must withstand the vibration, drops and abuse of a typical handset
  - Software – must be release controlled & compatible with the an existing operating system

UNCLASSIFIED



UNCLASSIFIED

QUALCOMM Government Technologies

## More details

- Power
  - Many power supplies operating at different voltages
  - Both linear and switching
  - Batteries 3.7V nominal, 3.2-4.2V range
  - Charged using linear charging from a 5V supply

### Sample Sensor Supply voltages

Vcc	Sensor Analog Circuit supply voltage	+2.85	+3.0	+3.15	V
Vdd_io	Sensor Digital I/O voltage	+1.62	+2.6	+3.63	V

### Sample Current Goals

Active	Sensing	-	5mA	-	mA
Standby	Standby	-	10uA	-	uA
Sleep	Sleep	-	1uA	-	uA

UNCLASSIFIED

# *Exhibit*

# 12

**UNITED STATES DISTRICT COURT  
FOR THE  
DISTRICT OF SOUTH CAROLINA – GREENVILLE**

RECEIVED  
USDC CLERK, GREENVILLE, SC  
2021 JAN 26 AM 10:13

LARRY GOLDEN,

Plaintiff,

V.

GOOGLE LLC

Defendants.

CIVIL CASE NO: \_\_\_\_\_

**JURY TRIAL DEMANDED**

January 25, 2021

**COMPLAINT FOR PATENT INFRINGEMENT**

This is an action of patent infringement in which plaintiff, Larry Golden (“Golden”, “Plaintiff” or “Patent Owner”), hereby asserts the following claims for patent infringement of United States Patent Nos. 10,163,287 (‘287 Patent), 9,589,439 (‘439 Patent), and 9,096,189 (‘189 Patent) (“patents-in-suit”: attached hereto as Exhibits A-C respectively) against Defendant GOOGLE LLC (“Google” or “Defendant”), and alleges as follows:

Upon information and belief, Plaintiff alleges the patents-in-suit, that were issued with the presumption of validity, “[a] patent shall be presumed valid. Each claim of a patent (whether in independent, dependent, or multiple dependent form) shall be presumed valid independently of the validity of other claims; dependent or multiple dependent claims shall be presumed valid even though dependent upon an invalid claim. 35 U.S. Code § 282 - Presumption of validity; (a)

In General” is Plaintiff’s evidence that the Plaintiff is the inventor of the Communicating, Monitoring, Detecting, and Controlling (CMDC) device(s) i.e., products grouped and commercialized today as smartphones, laptops, tablets, smartwatches, etc.

Upon information and belief, Plaintiff alleges that the defendant Google, has in the past and continues to do so, makes, uses, offer to sell, or sells Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), and 5, that Plaintiff believes infringes at least one of the claims in the patents-in-suit under 35 U.S.C. § 271, “anyone who makes, uses, offers to sell, or sells any patented invention domestically, or imports a patented invention into the United States during the term of the patent, is infringing the patent. Anyone who actively induces someone else to infringe the patent is also liable as an infringer.”

Similarly, under 35 U.S.C. § 271, “anyone who offers to sell, sells, or imports a material component of something that is patented, knowing that the component was especially made for use in an infringement and is not a commodity suitable for a substantial non-infringing use, is also liable as a contributory infringer” Plaintiff is alleging that the defendant Google, has in the past and continues to do so, offer to sell, sells (i.e., to other smartphone and mobile device manufacturers; “Google Search”, “Google Fi”, “Google Android Operating Systems”, “Google Cloud”, etc.) or imports a material component of something that is patented (i.e., Plaintiff’s CMDC devices). For example, “market.us” has published the following information on Google:

**2018?**

- On January 2018, Alphabet, Inc. acquired Redux – smartphone technology, which is specialized in turning smartphone screens into speakers.
- In October 2018, Google LLC to shut down Google+ after failing to disclose user data leak
- In November 2018, Google LLC acquired Workbench, which is a US-based company, that offers an online library of projects and lessons.



- Under this acquisition, the company focuses on integrating the Workbench tool with Google Classroom. In addition, currently, Google Classroom is one of the most widely used online educational tools, which lets parents, teachers, and students manage class discussions, assignments, and quizzes.
- In 2018, Google Search and Advertising tools helped generating **\$335 billion** in economic activity for **more than 1.3 billion** millions of businesses, website publishers, and nonprofits across the United States.
- Many website publishers, non-profit organizations and 40,000 companies in the country benefited from the use of Google Ads and AdSense advertising tools.
- In 2018, Google had sent more than 14 billion dollars to music publishers around the world.
- As of November, 2018, in US, Google connects people to businesses nearby more than **9 billion times**, including over 1 billion phone calls and 3 billion direction requests to stores every month.

#### Usage Statistics

- In a minute on the Internet in 2020, there are **4.1 million search queries**, **230 million per hour** and **6 Billion per day** that is **more than 2.5 Trillion searches per year** worldwide.
- Till July 2020, Google has 95.6% share of worldwide mobile search traffic.
- In April 2020, Google processed **12.7 billion** search queries in US, accounting **62.3 percent** of the US total desktop search queries and leading mobile search provider in the US with 95.04% market share
- Daily visitors to Google are **approximately 620 Mn.**
- According to the Datareportal, in June 2020, the top 10 search queries on Google were: Google, Facebook, Youtube, You, Weather, News, Amazon, Coronavirus, Translate and Instagram.
- In July 2019, Google accounted for **95 percent** of US mobile search visits and **93 percent** of overall U.S. organic search engine visits.
- As of May 2019, Gmail is a product that **1.5 billion users** rely on, to get things done every day.
- As of September 2019, People have already asked **Google Lens more than a billion questions** about things they see.

- Google sends **10 billion+ clicks per month** to news publishers' websites.
- As of May 2019, **2.5 million** web publishers use AdSense to make money through their content on the web.
- According to a survey, in Europe the news content linked through Google were **clicked more than 8 billion times a month** that is **3,000 clicks per second** to the publishers' websites in Europe resulting to each click between 4-6 euro cents.
- In the US, Google helps drive over **1 billion direct connections**, like calls and online reservations, for businesses nationwide every month.
- Google owns its **own common misspellings domains** such as [www.gooogle.com](http://www.gooogle.com), [www.googlr.com](http://www.googlr.com), and [www.gogle.com](http://www.gogle.com)
- Google runs **over 1 Mn computer servers** in data centers around the world.
- Last year, Google **rejected more than 10 million ads** that we suspected of copyright infringement.
- Around **35% of clicks** for U.S. businesses, advertising on Google, came from outside the country.
- As of May 2019, about **80% of traffic** from Google's Showcase Shopping ads to retailer sites are from new visitors discovering the brands.
- Till date, Google has over **2 billion store** offers mapped to physical store locations globally, discoverable by their current local ad formats like local inventory ads.
- Google Station serves more than **10 million people in 1,300 locations** across India, Indonesia, Mexico, Nigeria, the Philippines, Thailand, Vietnam and Brazil.
- Google Assistant is now on **more than one billion devices**, available in more than 30 languages across 80 countries.
- As of 2019, **more than 20 million people visit Google Account every day** to review their settings, using Privacy Checkup.
- As of 2019, **90 million** teachers and students are using G Suite for Education worldwide.
- Google has a database of over 4 billion credentials that have been compromised through various data breaches
- According to a 2018 Survey, around **72% of consumers in Indonesia** see Google Search as the online gateway for personal loan information and the second most helpful source for Financial Services information, after the bank branches

## THE PARTIES

1. Plaintiff Larry Golden is a citizen of South Carolina and has a principal place of business and residence at 740 Woodruff Road, #1102, Greenville, S.C. 29607.

2. On information and belief, Google is incorporated in the State of Delaware with a principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and does business in this judicial district by, among other things, committing jointly, directly, and/or indirectly the tort of literal patent infringement or infringement under the “doctrine of equivalents” giving rise to this complaint. Google may be served at its principal place of business at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

3. Google LLC is one of the largest technology companies in the world and conducts product sales, and online search operations in the District of South Carolina. Google LLC directly and/or indirectly distributes, markets, offers to sell, sells, and/or imports the infringing Google Pixel Series of smartphones and Google Android Operating Systems.

## STANDARD FOR REVIEW

4. Pursuant to the order of Magistrate Judge Kevin McDonald in United States District Court for the District of South Carolina; filed 12/17/2020; Case No. 6:20-cv-04353-BHH-KFM, Plaintiff was ordered to file “a short and plain statement of the claim showing that the pleader [Plaintiff] is entitled to relief.” Fed. R. Civ. P. 8(a).

5. Plaintiff has attached a copy of the asserted patents as **Exhibits A, B, & C**. The attached patents satisfy the requirement of “enough factual allegations. For example, in *Incom Corp. v. Walt Disney Co.*, No. 2:15-cv-03011-PSG-MRW, Dkt. 39, at \*4 (C.D. Cal. Feb. 4, 2016) the Central District of California declined to dismiss a complaint that attached the asserted

patent, identified the accused products by name, and generally compared the technology disclosed in the patents to the accused products. The complaint *did not identify any specific asserted claim*, but the court found that: “Plaintiff has stated a plausible claim for direct infringement by specifically identifying the Defendant’s products and alleging that they perform the same unique function as Plaintiff’s patented system.” The Defendant in this case is allegedly liable for infringement of the asserted patents-in-suit under 35 U.S.C. § 271.

6. Plaintiff maintains he has additional factual allegations to support his claim in the form claim charts readily available by order of this Court.

## JURISDICTION AND VENUE

7. This is a civil action for patent infringement arising under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1332(a) and 1338(a).

8. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, the defendant has purposely transacted business in this judicial district and has committed acts of joint, direct and/or indirect infringement in this judicial district.

9. On information and belief, the defendant is subject to this Court’s specific and general personal jurisdiction, due at least to the defendant’s substantial business in this forum, including: (A) at least part of the defendant’s infringing activities alleged herein, and (B) regularly doing or soliciting business, engaging in others persistent causes of conduct, and/or deriving substantial revenue from goods and services provided to persons and other entities in

South Carolina and this judicial district. The defendant has allegedly used, sold, and/or offered products for sale in South Carolina and is licensed to do business in this state.

10. This Court has specific jurisdiction over the defendant because the defendant has committed acts giving rise to this action and has established minimum contacts within this judicial district such that the exercise of jurisdiction over the defendant would not offend traditional notions of fair play and justice.

### RELATED CASES

11. Plaintiff has alleged that Apple is infringing Plaintiff's communicating, monitoring, detecting, and controlling (CMDC) device in a related case *Larry Golden v. Apple, Inc. et al* filed on 12/16/2020 at the United States District Court for the District of South Carolina; Greenville Division (Case No. 6:20-cv-04353) against defendants, Apple Inc. ("Apple"), Samsung Electronics, USA ("Samsung"), LG Electronics, USA, Inc. ("LG"), Qualcomm Inc. ("Qualcomm"), Motorola Solutions Inc. ("Motorola"), Panasonic Corporation ("Panasonic"), AT&T Inc. ("AT&T"), Verizon Corporation Services Group ("Verizon"), Sprint Corporation ("Sprint"), T-Mobile USA, Inc. ("T-Mobile"), Ford Global Technologies, LLC ("Ford"), Fairway Ford Lincoln of Greenville ("Fairway Ford"), General Motors Company ("GM"), Kevin Whitaker Chevrolet ("Whitaker Chevrolet"), FCA US LLC ("FCA"), and Big O Dodge Chrysler Jeep Ram ("Big O").

12. Plaintiff has filed an action of Antitrust Law violations *Larry Golden v. Apple, Inc. et al* on June 16, 2020, at the United States District Court for the District of South Carolina; Greenville Division (Case No. 6:20-cv-02270) against defendants, Apple Inc. ("Apple"), Samsung Electronics, USA ("Samsung"), LG Electronics, USA, Inc. ("LG"), Qualcomm Inc.

(“Qualcomm”), Ford Global Technologies, LLC (“Ford”), General Motors Company (“GM”), and, FCA US LLC (“FCA”).

## **GOOGLE SMARTPHONE SPECIFICATIONS / ANDROID PLATFORM**

13. Upon information and belief, Google is directly infringing Plaintiff’s patented CMDC devices by making, using, offering for sale, selling and/or importing the aforementioned alleged infringing devices that have at a minimum, directly infringed Plaintiff’s ‘287, ‘439, and ‘189 patents. to unjustly enrich itself.

14. Upon information and belief, Google is jointly infringing Plaintiff’s patented CMDC devices by offering for use, using, offering for sale, selling and/or importing as essential, Google’s Android platform for use with Google’s smartphones, and other Android smartphone devices i.e., Samsung, LG, Motorola, etc., that have at a minimum, directly infringed Plaintiff’s ‘287, ‘439, and ‘189 patents. Android smartphones have permanent default Google-owned apps like Google search, Google Play, YouTube, Maps etc. The main Android framework is signed in through a Google account too. So, you need to have a Google account to use Android.

15. The smartphone has come a long way since the first iPhone launched in 2007. While Apple’s iOS is arguably the world’s first smartphone operating system, Google’s Android is by far the most popular. Android has evolved significantly since first being released on an HTC-made T-Mobile device in 2008.

16. It wasn’t until 2005 that Google purchased Android, Inc., and while there wasn’t much info about Android at the time, many took it as a signal that Google would use the platform to enter the phone business. Eventually, Google did enter the smartphone business — but not as a hardware manufacturer. Instead, it marketed Android to other manufacturers, first

catching the eye of HTC, which used the platform for the first Android phone, the HTC Dream, in 2008.

17. Upon information and belief, Google has copied the “product grouping” strategy of the Plaintiff (Golden) for a communicating, monitoring, detecting, and controlling (CMDC) device, i.e., Google’s smartphone products are grouped together by “common features of design similarities”. As illustrated below, Google’s smartphones are basically the same.

18. Therefore, when analyzing the specifications, features, and functionality of Google’s smartphones as a complete product, and not merely identifying the individual infringing processes; there is a strong likelihood that if one of Google’s smartphones infringes Plaintiff’s claimed invention of a CMDC device; it can be perceived that all of Google’s smartphones infringes Plaintiff’s claimed invention of a CMDC device as a ‘whole’ product.

#### GOOGLE PIXEL 5 VS. PIXEL 4A WITH 5G VS. PIXEL 4

Category	Pixel 5	Pixel 4A with 5G	Pixel 4A
Network	5G	5G	4G
Screen	6-inch flexible OLED display at 432 ppi	6.2-inch OLED display at 413 ppi	5.8-inch OLED display at 443 ppi
Refresh Rate	90 Hz	60 Hz	60 Hz
Resolution	1080 x 2340	1080 x 2340	1080 x 2340
Battery	4080 mAh	3885 mAh	3140 mAh
Front Camera	8 megapixels	8 megapixels	8 megapixels
Rear Camera	12.2-megapixel dual-pixel (16-megapixel ultrawide)	12.2-megapixel dual-pixel (16-megapixel ultrawide)	12.2-megapixel dual-pixel
Camera Features	Night Sight, Portrait Light, Cinematic Pan, Live HDR+	Night Sight, Portrait Light, Cinematic Pan, Live HDR+	Night Sight, Live HDR+
RAM	8GB	6GB	6GB

Category	Pixel 5	Pixel 4A with 5G	Pixel 4A
<b>Processor</b>	Qualcomm Snapdragon 765G	Qualcomm Snapdragon 765G	Qualcomm Snapdragon 730G
<b>Storage</b>	128GB	128GB	128GB
<b>Audio</b>	Stereo speakers, USB-C audio	Stereo speakers, USB-C audio, 3.5mm headphone jack	USB-C audio, 3.5mm headphone jack
<b>Price</b>	\$699	\$499	\$349
<b>Wireless Charging</b>	Yes	No	No
<b>Water Resistant</b>	Yes	No	No
<b>Colors</b>	Green, Black	White, Black	Black
<b>Operating System</b>	Pre-loaded with Android 11	Pre-loaded with Android 11	Pre-loaded with Android 10

#### GOOGLE PIXEL 3 SERIES SPEC COMPARISON

Specification	Pixel 3A	Pixel 3A XL	Pixel 3	Pixel 3 XL
<b>Display</b>	5.6 inches	6.0 inches	5.5 inches	6.3 inches
<b>Resolution</b>	2220 x 1080	2160 x 1080	2160 x 1080	2960 x 1440
<b>Processor</b>	Snapdragon 670 (2.0GHz and 1.7GHz, octa-core)	Snapdragon 670 (2.0GHz and 1.7GHz, octa-core)	Snapdragon 845 (2.5GHz and 1.6GHz, octa-core)	Snapdragon 845 (2.5GHz and 1.6GHz, octa-core)
<b>RAM</b>	4GB	4GB	4GB	4GB
<b>Storage</b>	64GB	64GB	64GB, 128GB	64GB, 128GB
<b>Rear camera</b>	12 megapixels	12 megapixels	12 megapixels	12 megapixels
<b>Front camera</b>	8 megapixels	8 megapixels	8 megapixels, 8 megapixels(wide)	8 megapixels, 8 megapixels(wide)



<b>Specification</b>	<b>Pixel 3A</b>	<b>Pixel 3A XL</b>	<b>Pixel 3</b>	<b>Pixel 3 XL</b>
<b>Battery</b>	3,000mAh	3,700mAh	2,915mAh	3,430mAh
<b>Water protection</b>	N/A	N/A	IPX8	IPX8
<b>Wireless charging?</b>	No	No	Yes	Yes
<b>Ports?</b>	USB-C, 3.5mm headphone jack	USB-C, 3.5mm headphone jack	USB-C	USB-C
<b>Weight</b>	0.32 pounds	0.37 pounds	0.33 pounds	0.4 pounds
<b>Dimensions (in.)</b>	6.0 x 2.80 x 0.30	6.30 x 3.00 x 0.30	5.70 x 2.70 x 0.30	6.20 x 3.00 x 0.30
<b>Starting price</b>	\$399.00	\$479.00	\$799.00	\$899.00
<b>Operating System</b>	Pre-loaded Android	Pre-loaded Android	Pre-loaded Android	Pre-loaded Android

#### SENSOR TYPES SUPPORTED BY THE “*ANDROID*” PLATFORM

<b>Type Accelerometer</b>	Hardware	Measures the acceleration force in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, and z), including the force of gravity.	Motion detection (shake, tilt, etc.).
<b>Type Ambient Temperature</b>	Hardware	Measures the ambient room temperature in degrees Celsius (°C). See note below.	Monitoring air temperatures.
<b>Type Gravity</b>	Software or Hardware	Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z).	Motion detection (shake, tilt, etc.).
<b>Type Gyroscope</b>	Hardware	Measures a device's rate of rotation in rad/s around each of the three physical axes (x, y, and z).	Rotation detection (spin, turn, etc.).
<b>Type Light</b>	Hardware	Measures the ambient light level (illumination) in lx.	Controlling screen brightness.

<b>Type Linear Acceleration</b>	Software or Hardware	Measures the acceleration force in $m/s^2$ that is applied to a device on all three physical axes (x, y, and z), excluding the force of gravity.	Monitoring acceleration along a single axis.
<b>Type Magnetic Field</b>	Hardware	Measures the ambient geomagnetic field for all three physical axes (x, y, z) in $\mu T$ .	Creating a compass.
<b>Type Orientation</b>	Software	Measures degrees of rotation that a device makes around all three physical axes (x, y, z). As of API level 3 you can obtain the inclination matrix and rotation matrix for a device by using the gravity sensor and the geomagnetic field sensor in conjunction with the <code>getRotationMatrix()</code> method.	Determining device position.
<b>Type Pressure</b>	Hardware	Measures the ambient air pressure in hPa or mbar.	Monitoring air pressure changes.
<b>Type Proximity</b>	Hardware	Measures the proximity of an object in cm relative to the view screen of a device. This sensor is typically used to determine whether a handset is being held up to a person's ear.	Phone position during a call.
<b>Type Relative Humidity</b>	Hardware	Measures the relative ambient humidity in percent (%).	Monitoring dewpoint, absolute, and relative humidity.
<b>Type Rotation Vector</b>	Software or Hardware	Measures the orientation of a device by providing the three elements of the device's rotation vector.	Motion detection and rotation detection.
<b>Type Temperature</b>	Hardware	Measures the temperature of the device in degrees Celsius ( $^{\circ}C$ ). This sensor implementation varies across devices and this sensor was replaced with the <b>Type—Ambient Temperature</b> sensor in API Level 14	Monitoring temperatures.

- ❖ **BIOMETRICS:** Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).
- ❖ **DISABLING LOCK MECHANISM:** Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. When setting the pattern, you must drag your finger along lines on the screen between different nodes. Afterward, to unlock the phone, you'll need to replicate the pattern drawn. If you fail to solve the

pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account. If you can't log in, you'll have to employ some other methods to restore control of your phone.

- ❖ **CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) DETECTION:** Through collaboration and innovation, the Defense Threat Reduction Agency has integrated its powerful, hazard-awareness-and-response tools into the *Android Tactical Assault Kit (or the Android Team Awareness Kit, ATAK)*. ATAK is a digital application available to warfighters throughout the DoD. Built on the Android operating system, ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.
  - ❖ **HEART RATE:** *Android Team Awareness Kit, ATAK* provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.
  - ❖ **NEAR FIELD COMMUNICATION (NFC):** Pixel™, Phone by Google - Turn NFC on/off. Near Field Communication (NFC) allows the transfer of data between devices that are a few centimeters apart, typically back-to-back. NFC must be turned on for NFC-based apps (e.g., Tap to Pay) to function correctly. NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. NFC allows you to share small payloads of data between an NFC tag and an Android-powered device, or between two Android-powered devices. Tags can range in complexity.
  - ❖ **WARFIGHTERS:** The U.S. armed forces and their interagency and coalition partners value *Android Team Awareness Kit, ATAK* and the common operating picture it provides. DTRA continues to develop CBRN-specific plug-in capabilities to support warfighters on the battlefield.
- 

## GOOGLE'S JOINT INFRINGEMENT WITH APPLE INC.

19. According to Gurman, 2020, "The U.S. government's antitrust assault against Google reveals new details about a secretive, multibillion-dollar deal between the internet giant and Apple Inc., the world's largest technology company. The Justice Department's lawsuit, filed Tuesday, targets paid deals Google negotiates to get its search engine to be the default on browsers, phones and other devices. The biggest of these is an agreement that makes Google search the default on iPhones and other Apple devices."

20. The U.S. government said Apple Chief Executive Officer Tim Cook and Google CEO Sundar Pichai met in 2018 to discuss the deal. After that, an unidentified senior Apple employee wrote to a Google counterpart that “our vision is that we work as if we are one company.”

21. The DOJ also cited internal Google documents that call the Apple search deal a “significant revenue channel” for the search giant and one that, if lost, would result in a “Code Red” scenario. That’s because nearly half of Google search traffic in 2019 came from Apple products, according to the lawsuit.

22. Google pays Apple billions of dollars a year to make its search product the default option, according to analyst estimates. That means when a user buys a new iPhone or other Apple device, the built-in search engine in the Safari browser is Google.

23. The DOJ suit cited estimates that Apple gets \$8 billion to \$12 billion annually from Google through the agreement. Apple’s income from the search deal is believed to be part of the company’s growing Services segment, a key metric Apple has highlighted to investors and analysts in recent years.

Gurman, Mark (2020, Oct. 20). *Apple, Google worked as ‘one company’ on search deal, U.S. says*. <https://www.bloomberg.com/news/articles/2020-10-20/apple-google-worked-as-one-company-on-search-deal-u-s-says>

### **Joint Infringement**

24. Upon information and belief, Google and Apple are jointly infringing Plaintiff’s patented CMDC devices by offering for use, using, offering for sale, selling and/or importing as essential, Google’s Search for use with Google and Apple smartphones, that have at a minimum, directly infringed independent claims 1, 2, and 3 of the ‘189 patent; independent claims 13, 14, 15, and 23 of the ‘439 patent; and, independent claims 4, 5, and 6 of the ‘287 patent.

25. Plaintiff has alleged that Apple is infringing Plaintiff's communicating, monitoring, detecting, and controlling (CMDC) device in a related case *Larry Golden v. Apple, Inc. et al* filed on 12/16/2020 at the United States District Court for the District of South Carolina; Greenville Division (Case No. 6:20-cv-04353) against defendants, Apple Inc. et al.

26. Plaintiff has also filed a case *Larry Golden v. Apple, Inc. et al* on 06/16/2020 at the United States District Court for the District of South Carolina; Greenville Division (Case No. 6:20-cv-02270) against defendants, Apple Inc. et al. for Antitrust Law Violations.

### **GOOGLE'S JOINT INFRINGEMENT WITH QUALCOMM INC.**

27. According to a Qualcomm press release (2020), "Qualcomm Technologies, Inc. and Google announced their collaboration to enhance and extend Project Treble with the goal of enabling more devices with Qualcomm® Snapdragon™ mobile platforms to run the latest Android OS. The enhancements are intended to enable Original Equipment Manufacturers (OEMs) to upgrade their Snapdragon based devices to the latest Android OS without modifying Qualcomm Technologies' chipset-specific software and to use a common Android software branch to upgrade devices based on a wide range of Snapdragon mobile platforms across Qualcomm Technologies' portfolio. These enhancements are designed to reduce the time and resources required to upgrade Snapdragon based devices to the latest Android OS version."

28. As part of this collaboration with Google, Qualcomm Technologies will now support four Android OS versions and four years of security updates for all Snapdragon platforms utilizing the Project Treble enhancements, starting with the new Snapdragon 888 Mobile Platform. These initiatives are designed to enable faster Android OS upgrades with fewer resources and a predictable software lifecycle for Snapdragon based devices, which together are

expected to result in more consumers with Snapdragon based devices running the latest Android OS version.

29. “Google continues to work closely with our technology partners to increase the freshness of the Android ecosystem. Through this collaboration with Qualcomm Technologies, we expect that Android users will have the latest OS upgrades and greater security on their devices,” said David Burke, vice president of Android engineering, Google.

30. “We are excited to work with Google to extend our support for Android OS and security updates on future Snapdragon mobile platforms utilizing the Project Treble enhancements,” said Kedar Kondap, vice president, product management, Qualcomm Technologies, Inc.

#### **Terminology**

- Google’s android operating system; same as “operating system”.
- Google’s android operating system; same as “computer program”.
- Google’s android operating system; same as “software”.
- Qualcomm’s chipset; used interchangeably as “processor”.
- Qualcomm’s chipset; used interchangeably as “central processing unit”.
- Qualcomm’s chipset; used interchangeably as “wireless technology” (WiFi, 3G, 4G, 5G, LTE, and so on).

31. An operating system is a computer program, works as interface between user and hardware and provides common services for computer programs. The entire process or functionality of computer system depends on the operating system. An operating system is a computer program that controls the execution of application programs and acts as an interface between the user of a computer and the computer hardware. The purpose of an operating system

is to provide an environment in which a user can execute programs in a convenient and efficient manner. <https://www.geeksforgeeks.org/introduction-of-operating-system-set-1/>

32. A Central Processing Unit (CPU) is a machine that can execute computer programs. This broad definition can easily be applied to many early computers that existed long before the term "CPU" ever came into widespread usage. The term itself and its initialism have been in use in the computer industry at least since the early 1960s (Weik 1961). The form, design and implementation of CPUs have changed dramatically since the earliest examples, but their fundamental operation has remained much the same.

33. An Operating System is the core software that allows applications to interface with the hardware. Operating Systems control the specific details of your system, presenting a more manageable interface for applications (and the user) to make use of. To use an analogy, the CPU is the brain, the OS is the mind. The mind cannot exist without a brain to store it, and the brain is just a useless lump without a mind to control it.

<https://answers.yahoo.com/question/index?qid=20090927101607AAiAJ42>

34. An SoC, or system-on-a-chip to give its full name, integrates almost all of these components into a single silicon chip. Along with a CPU, an SoC usually contains a GPU (a graphics processor), memory, USB controller, power management circuits, and wireless radios (WiFi, 3G, 4G LTE, and so on). Whereas a CPU cannot function without dozens of other chips, it's possible to build complete computers with just a single SoC. The number one advantage of an SoC is its size: An SoC is only a little bit larger than a CPU, and yet it contains a lot more functionality. If you use a CPU, it's very hard to make a computer that's smaller than 10cm (4 inches) squared, purely because of the number of individual chips that you need to squeeze in. Using SoCs, we can put complete computers in smartphones and tablets, and still have plenty of

space for batteries. <https://www.extremetech.com/computing/126235-soc-vs-cpu-the-battle-for-the-future-of-computing>.

### **Joint Infringement**

35. Upon information and belief, Google and Qualcomm are jointly infringing Plaintiff's patented CMDC devices by offering for use, using, offering for sale, selling and/or importing as essential, Google's Android platform for use with Qualcomm's SoCs, CPUs, etc. for smartphones that have at a minimum, directly infringed independent claims 1, 2, and 3 of the '189 patent; independent claims 13, 14, 15, and 23 of the '439 patent; and, independent claims 4, 5, and 6 of the '287 patent.

36. Google developing its own phone processor would mean dumping the Qualcomm SoCs it usually uses. Of course, you can never truly be rid of Qualcomm: Google would presumably still need to use Qualcomm modems, something that even Apple still needs to do. There are other modem manufacturers out there—Samsung, Huawei, Mediatek—but Qualcomm's combination of patents and strong-arm licensing techniques has effectively locked its competitors out of the US and other markets.

37. Plaintiff has alleged that Qualcomm is infringing Plaintiff's communicating, monitoring, detecting, and controlling (CMDC) device in a related case *Larry Golden v. Apple, Inc. et al.* filed on 12/16/2020 at the United States District Court for the District of South Carolina; Greenville Division (Case No. 6:20-cv-04353) against defendants, *Apple Inc. et al.*

38. Plaintiff has also filed a case *Larry Golden v. Apple, Inc. et al* on 06/16/2020 at the United States District Court for the District of South Carolina; Greenville Division (Case No. 6:20-cv-02270) against defendants, *Apple Inc. et al.* for Antitrust Law Violations.



## CLAIM CONSTRUCTION

*“Inter Partes Review (IPR): Department of Homeland Security vs. Larry Golden; Case No.: IPR2014-00454 (Patent RE43,990; Claims 11, 74, & 81); Final Written Decision entered on October 1, 2015. “In the ‘Decision to Institute’, we construed certain claim terms. Those constructions are reproduced in the chart below:*

Claim Term	Construction
“built in, embedded” (claim 74)	“something is included within, incorporated into, disposed within, affixed to, connected to, or mounted to another device, such that it is an integral part of the device”
“communication device” (claim 81)	“monitoring equipment”

Dec. to Inst. 11-16

39. “No party challenges these constructions. Both of these terms were modified or removed in the amendment. To the extent that any of these constructions remain relevant after the amendment, we see no reason to modify them... [w]e further determined that no explicit construction was necessary for any other claim terms. Dec. to Inst. 10-11. Based on the record adduces during trial, we see no need to construe any other terms...”

40. “Beginning with the claim preamble amendment, the preamble of claim 11 originally read: “A communication device of at least one of *a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal at a monitoring site* for monitoring products for communication therebetween, comprising....” In claim 154, the language in italics has been eliminated and replaced with “the products grouped together by common features in the product grouping category of design similarity (e.g., computer terminal, personal computer (PC)) ...” Patent Owner contends that this new language is consistent with

words found in the disclosure of the ‘118 application. Mot. To Amend 4. Patent Owner further contends that this new language is broad enough to include the removed items, such as cell phones and smart phones, because those items are “species terms” that are “included in the genus ‘monitoring equipment’ and ‘communication device’ when the clause ‘products grouped together by common features in the product groupings category of design similarity’ is included.” *Id.* Patent Owner argues that “[t]he specific devices removed, such as the cell phones and smart phones would be recognized by one of ordinary skill in the art as a type of communication device or monitoring equipment because cell phones and smartphones are devices that are capable of communication and are capable of receiving signals.” *“Inter Partes Review (IPR): Department of Homeland Security vs. Larry Golden; Case No.: IPR2014-00454 (Patent RE43,990; Claims 11, 74, & 81); Final Written Decision entered on October 1, 2015.*

## COUNT I

### (Infringement of the ‘287 Patent)

41. Golden realleges and incorporates herein the allegations set forth in Paragraphs 1-40.

42. On information and belief, Google is jointly, directly, indirectly and/or under the ‘doctrine of equivalents’, infringing at least independent claims 4, 5, and 6 of the ‘287 patent. The alleged infringing products are: Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), and 5.

43. As set forth in Golden’s preliminary infringement contentions that Google is making, using, offering for sale, selling and/or importing Plaintiff’s CMDC device have at a minimum directly infringed the ‘287 patent and Google is thereby liable for infringement of the

‘287 patent pursuant to 35 U.S.C. § 271. Google have caused damage to Golden, which infringement and damage will continue unless and until Google is enjoined.

44. The alleged infringement of Golden identified in this Count has caused irreparable injury to Golden for which remedies at law are inadequate. Considering the balance of the hardships between the parties, a remedy in equity, such as a permanent injunction is warranted and such a remedy would be in the public interest.

## **COUNT II**

### **(Infringement of the ‘439 Patent)**

45. Golden realleges and incorporates herein the allegations set forth in Paragraphs 1-44.

46. On information and belief, Google is jointly, directly, indirectly and/or under the ‘doctrine of equivalents’, infringing at least independent claims 13, 14, 15, and 23 of the ‘439 patent. The alleged infringing products are: Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), and 5.

47. As set forth in Golden’s preliminary infringement contentions that Google is making, using, offering for sale, selling and/or importing Plaintiff’s CMDC device have at a minimum directly infringed the ‘439 patent and Google is thereby liable for infringement of the ‘439 patent pursuant to 35 U.S.C. § 271. Google have caused damage to Golden, which infringement and damage will continue unless and until Google is enjoined.

48. The alleged infringement of Google identified in this Count has caused irreparable injury to Golden for which remedies at law are inadequate. Considering the balance of the hardships between the parties, a remedy in equity, such as a permanent injunction is warranted and such a remedy would be in the public interest.

### **COUNT III**

#### **(Infringement of the ‘189 Patent)**

49. Golden realleges and incorporates herein the allegations set forth in Paragraphs 1-48.


50. On information and belief, Google is jointly, directly, indirectly and/or under the ‘doctrine of equivalents’, infringing claims 1, 2 & 3 of the ‘189 patent. The alleged infringing products are: Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), and 5.

51. As set forth in Golden’s preliminary infringement contentions that Google is making, using, offering for sale, selling and/or importing Plaintiff’s CMDC device have at a minimum directly infringed the ‘189 patent and Google is thereby liable for infringement of the ‘189 patent pursuant to 35 U.S.C. § 271. Google have caused damage to Golden, which infringement and damage will continue unless and until Google is enjoined.

52. The alleged infringement of Google identified in this Count has caused irreparable injury to Golden for which remedies at law are inadequate. Considering the balance of the hardships between the parties, a remedy in equity, such as a permanent injunction is warranted and such a remedy would be in the public interest.

### **CLAIM CHART**

53. The following Claim Chart is an illustration of literal infringement. At least one of the alleged infringing products of Google (i.e., Google Pixel smartphones 3, 3XL, 3a, 3aXL, 4a, 4a(5G), or 5) is representative of all the alleged infringing products of Google asserted in this complaint. At least one of the alleged infringing products of Google (Google Pixel 5) is illustrated to show how the Google Pixel 5 allegedly infringes on at least one of the asserted independent claims of each of the patents-in-suit (‘287, ‘439, and ‘189 patents).

Google Pixel 5 Smartphone	Patent #: 10,163,287; Independent Claim 5	Patent #: 9,589,439; Independent Claim 23	Patent #: 9,096,189; Independent Claim 1
	A monitoring device, comprising:	A cell phone comprising:	A communication device of at least one of a cell phone, a smart phone, a desktop, a handheld, a PDA, a laptop, or a computer terminal for monitoring products, interconnected to a product for communication therebetween, comprising:
CPU: Octa-core (1 × 2.4 GHz Kryo 475 Prime & 1 × 2.2 GHz Kryo 475 Gold & 6 × 1.8 GHz Kryo 475 Silver) System-on-a-chip: Qualcomm Snapdragon 765G	at least one central processing unit (CPU);	a central processing unit (CPU) for executing and carrying out the instructions of a computer program;	at least one of a central processing unit (CPU) for executing and carrying out the instructions of a computer program, a network processor which is specifically targeted at the networking application domain, or a front-end processor for communication between a host computer and other devices;
Ambient Temperature sensor supported by the Android platform. Measures the ambient room temperature in degrees Celsius (°C). Monitoring air temperatures. Monitoring air temperatures.	at least one temperature sensor in communication with the at least one CPU for monitoring temperature;	X	X

Gravity sensor supported by the Android platform. Measures the force of gravity in m/s <sup>2</sup> that is applied to a device on all three physical axes (x, y, z). Motion detection (shake, tilt, etc.).	at least one motion sensor in communication with the at least one CPU;	X	X
Light sensor supported by the Android platform. Measures the ambient light level (illumination) in lx. Controlling screen brightness. Screen: 6-inch flexible OLED display at 432 ppi	at least one viewing screen for monitoring in communication with the at least one CPU;	X	X
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one global positioning system (GPS) connection in communication with the at least one CPU;	at least one of a satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long range radio frequency (RF) connection, short range radio frequency (RF) connection, or GPS connection;	at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection, long and short-range radio frequency (RF) connection, or GPS connection;
Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable	at least one of an internet connection or a Wi-Fi connection in communication with the at least one CPU;	wherein at least one of... WiFi connection, internet connection, radio frequency (RF) connection, cellular connection... capable of signal communication with the transmitter or the receiver;	wherein the only type or types of communication with the transmitter and the receiver of the communication device and transceivers of the products is a type or types selected from the group... of satellite, Bluetooth, WiFi...

<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one of a Bluetooth connection, a cellular connection, or a satellite connection in communication with the at least one CPU;</p>	<p>at least one of a... Bluetooth connection, WiFi connection, internet connection... cellular connection... short range radio frequency (RF) connection, or GPS connection;</p>	<p>X</p>
<p>Google's Android operating system features a lock mechanism to secure your phone, known as pattern lock. To set, drag your finger along lines on the screen. To unlock the phone, replicate the pattern drawn. If you fail to solve the pattern too many times, the phone locks and cannot be unlocked without logging into the associated Google account.</p> <p>Google Nest x Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p>	<p>at least one locking mechanism in communication with the at least one CPU for locking the communication device, the at least one locking mechanism configured to at least one of engage (lock) the communication device, disengage (unlock) the communication device, or disable (make unavailable) the communication device;</p>	<p>whereupon the cell phone is interconnected to the cell phone detection device to receive signals or send signals to lock or unlock doors, to activate or deactivate security systems, to activate or deactivate multi-sensor detection systems, or to activate or deactivate the cell phone detection device;</p>	<p>X</p>
<p>Pixel phones use USB-C with USB 2.0 power adapters and cables. To charge your phone with a USB-A power adapter, use a USB-C to USB-A cable.</p>	<p>at least one power source comprising at least one of a battery, electrical connection, or wireless connection, to provide power to the communication device;</p>	<p>X</p>	<p>X</p>

<p><b>BIOMETRICS:</b> Biometric factors allow for secure authentication on the Android platform. The Android framework includes face and fingerprint biometric authentication. Android can be customized to support other forms of biometric authentication (such as Iris).</p>	<p>at least one biometric sensor in communication with the at least once CPU for providing biometric authentication to access the communication device;</p>	<p>wherein the cell phone is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan, or signature such that the cell phone is locked by the biometric lock disabler to prevent unauthorized use; and</p>	<p>wherein the communication device is equipped with a biometric lock disabler that incorporates at least one of a fingerprint recognition, voice recognition, face recognition, hand geometry, retina scan, iris scan and signature such that the communication device that is at least one of the cell phone, the smart phone, the desktop, the handheld, the PDA, the laptop or the computer terminal is locked by the biometric lock disabler to prevent unauthorized use</p>
<p><i>Android Team Awareness Kit, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies, whether that is a wearable smartwatch that measures a warfighter's vitals (e.g., heart rate) or a device mounted on a drone to detect chemical warfare agents.</i></p>	<p>at least one sensor for chemical, biological, or human detection in communication with the at least one CPU;</p>	<p>the cell phone is at least a fixed, portable or mobile communication device interconnected to the cell phone detection device, capable of wired or wireless communication therebetween; and</p>	<p>the communication device is at least a fixed, portable or mobile communication device interconnected to a fixed, portable or mobile product, capable of wired or wireless communication therebetween...</p>



<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>one or more detectors in communication with the at least one CPU for detecting at least one of chemical, biological, radiological, or explosive agents;</p>	<p>at least one of a chemical sensor, a biological sensor, an explosive sensor, a human sensor, a contraband sensor, or a radiological sensor capable of being disposed within, on, upon or adjacent the cell phone;</p>	<p>wherein the communication device receives a signal via any of one or more products listed in any of the plurality of product grouping categories;</p>
<p>Connectivity: Wi-Fi 5 (a/b/g/n/ac) 2.4 + 5.0 GHz, Bluetooth 5.0 + LE, NFC, GPS (GLONASS, Galileo, BeiDou), eSIM capable</p>	<p>at least one radio-frequency near-field communication (NFC) connection in communication with the at least one CPU...</p>	<p>X</p>	<p>X</p>
<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	<p>at least one of a transmitter or a transceiver in communication with the at least one CPU configured to send signals to monitor at least one of a door, a vehicle, or a building, send signals to lock or unlock doors, send signals to control components of a vehicle, send signals to control components of a building, or... detect at least one of a chemical biological... agent such that the communication device is capable of communicating, monitoring, detecting, and controlling.</p>	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>a transmitter for transmitting signals and messages to at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p> <p>a receiver for receiving signals, data or messages from at least one of plurality product groups based on the categories of a multi-sensor detection device, a maritime cargo container, a cell phone detection device, or a locking device;</p>

<p>Google Nest × Yale Lock is connected to the Nest app; you can lock or unlock your door from your phone.</p> <p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) provides a single interface for viewing and controlling different CBRN-sensing technologies</p>	X	X	<p>whereupon the communication device, is interconnected to a product equipped to receive signals from or send signals to lock or unlock doors, activate or deactivate security systems, activate or deactivate multi-sensor detection systems, or to activate or deactivate cell phone detection systems</p>
<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA's contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	X	<p>a transmitter for transmitting signals and messages to a cell phone detection device; a receiver for receiving signals from the cell phone detection device;</p>	<p>wherein at least one satellite connection, Bluetooth connection, WiFi connection, internet connection, radio frequency (RF) connection, cellular connection, broadband connection... short range radio frequency (RF) connection is capable of signal communication with the transmitter and the receiver of the communication device and transceivers of the products;</p>

<p><i>Android Team Awareness Kit</i>, ATAK (built on the Android operating system) is a digital application available to warfighters throughout the DoD. ATAK offers warfighters geospatial mapping for situational awareness during combat — on an end-user device such as a smartphone or a tablet. With DTRA’s contribution, ATAK now includes chemical, biological, radiological, and nuclear (CBRN) plug-ins.</p>	<p>X</p>	<p>whereupon a signal sent to the receiver of the cell phone detection device from at least one of the chemical sensor, the biological sensor, the explosive sensor, the human sensor, the contraband sensor, or the radiological sensor, causes a signal that includes at least one of location data or sensor data to be sent to the cell phone.</p>	<p>X</p>
--	----------	--	----------

### PRAYER FOR RELIEF

Wherefore, Golden respectfully requests that this Court enter:

- A. A judgment in favor of Golden that the defendant has infringed at least one or more claims of the ‘287 Patent, the ‘439 Patent, and the ‘189 Patent as aforesaid;
- B. A permanent injunction enjoining the defendant, its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents and all others acting in active concert or privity therewith from direct, indirect and/or joint infringement of the ‘287, ‘439, and ‘189 patents as aforesaid pursuant to 35 U.S.C. § 283;
- C. A judgment and order requiring the defendant to pay Golden its damages with pre- and post-judgment interest thereon pursuant to 35 U.S.C. § 284;
- D. As set forth in Golden’s preliminary infringement contentions that the Defendant in this case is making, using, offering for sale, selling and/or importing the aforementioned


alleged infringing devices that have at a minimum, directly infringed the '287, '439, and '189 patents. The Defendant is thereby liable for infringement of the '287, '439, and '189 patents pursuant to 35 U.S.C. § 271. The Defendant has caused damage to Golden, which infringement and damage will continue unless and until the Defendant is enjoined.

E. Any and all further relief to which the Court may deem Golden entitled.

### **DEMAND FOR JURY TRIAL**

Golden requests a trial by jury on all issues so triable by right pursuant to Fed. R. Civ. P. 38. A right guaranteed under the Seventh Amendment of the Constitution.

Respectfully submitted,

S/  Date: 01 /25 /2021

Larry Golden, Petitioner, Pro Se

740 Woodruff Rd., #1102

Greenville, South Carolina 29607

(H) 864-288-5605 / (M) 864-992-7104

atpg-tech@charter.net


**UNITED STATES  
POSTAL SERVICE®**
**PRIORITY  
MAIL  
EXPRESS®**


EI 975 707 097 US

## CUSTOMER USE ONLY

FROM: (PLEASE PRINT)

PHONE

864 288-5605

LARRY GOLDEN  
740 WOODRUFF RD.  
#1102  
GREENVILLE, SC 29607

## DELIVERY OPTIONS (Customer Use Only)

☒ **SIGNATURE REQUIRED** Note: The mailer must check the "Signature Required" box if the mailer: 1) Requires the addressee's signature; OR 2) Purchases additional insurance; OR 3) Purchases COD service; OR 4) Purchases Return Receipt service. If the box is not checked, the Postal Service will leave the item in the addressee's mail receptacle or other secure location without attempting to obtain the addressee's signature on delivery.

## Delivery Options

- ☐ No Saturday Delivery (delivered next business day)  
☐ Sunday/Holiday Delivery Required (additional fee, where available\*)  
\*Refer to USPS.com® or local Post Office™ for availability.

TO: (PLEASE PRINT)

PHONE

202 275-8000

U.S. COURT OF APPEALS FOR THE FEDERAL  
CIRCUIT  
CASE No: 24-2256  
717 MADISON PLACE, NW  
WASHINGTON, DC

ZIP + 4® (U.S. ADDRESSES ONLY)

2 0 4 3 9 -

- For pickup or USPS Tracking™, visit USPS.com or call 800-222-1811.  
■ \$100.00 insurance included.

## PAYMENT BY ACCOUNT (if applicable)

Federal Agency Acct. No. or Postal Service™ Acct. No.

## ORIGIN (POSTAL SERVICE USE ONLY)

<input checked="" type="checkbox"/> 1-Day	<input type="checkbox"/> 2-Day	<input type="checkbox"/> Military	<input type="checkbox"/> DPO
PO ZIP Code	Scheduled Delivery Date (MM/DD/YY)	Postage	
29607	08/29/24	\$ 52.55	
Date Accepted (MM/DD/YY)	Scheduled Delivery Time	Insurance Fee	COD Fee
8/28/24	<input checked="" type="checkbox"/> 6:00 PM	\$	\$
Time Accepted	<input type="checkbox"/> AM <input checked="" type="checkbox"/> PM	Return Receipt Fee	Live Animal Transportation Fee
12:52		\$	\$
Special Handling/Fragile	Sunday/Holiday Premium Fee	Total Postage & Fees	
\$	\$	\$ 52.55	
Weight	<input type="checkbox"/> Flat Rate	Acceptance Employee Initials	
3 lbs. 3 ozs.		SS	

## DELIVERY (POSTAL SERVICE USE ONLY)

Delivery Attempt (MM/DD/YY)	Time	Employee Signature
	<input type="checkbox"/> AM <input type="checkbox"/> PM	
Delivery Attempt (MM/DD/YY)	Time	Employee Signature
	<input type="checkbox"/> AM <input type="checkbox"/> PM	


**PEEL FROM THIS CORNER**